

CPNI

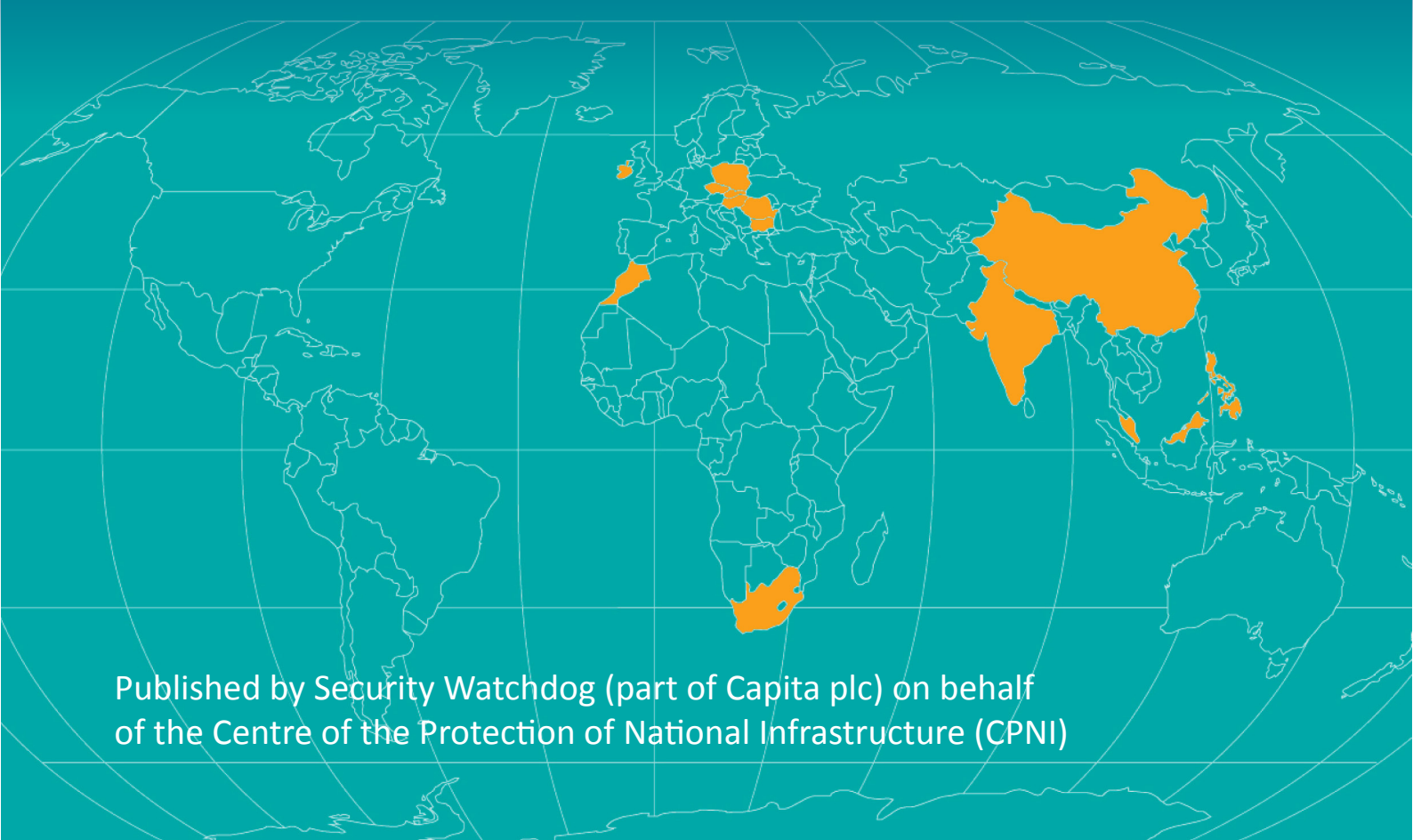
Centre for the Protection
of National Infrastructure

SECURITY

WATCHDOG
Part of Capita plc

Personnel Security in Offshore Centres

● April 2014

A world map with a grid overlay. Several regions are highlighted in orange: parts of Europe (including the UK, France, and Germany), parts of Africa (including Egypt, Sudan, and South Africa), India, China, and parts of Southeast Asia (including the Philippines, Indonesia, and Malaysia).

Published by Security Watchdog (part of Capita plc) on behalf
of the Centre of the Protection of National Infrastructure (CPNI)

Contents



Executive Summary

Bulgaria

Morocco

China

Philippines

Czech Republic

Poland

Hungary

Romania

India

Singapore

Ireland

Slovakia

Malaysia

South Africa

Important Notice

Disclaimer

We have been instructed by the Centre for the Protection of National Infrastructure (CPNI) to undertake confirmatory research into personnel security measures in a number of popular offshoring and outsourcing locations worldwide.

The information contained in this report reflects previous studies commissioned by CPNI which have been updated and was compiled during November 2013 – February 2014. This information should be considered current as at the date the research was undertaken.

This report was prepared for CPNI. Capita plc does not assume any responsibility to any other party in respect of this report or any judgments, conclusions, opinions, findings or recommendations that Capita plc may have formed or made and, to the fullest extent permitted by law, Capita plc will accept no liability in respect of any such matters to any third party. Should you choose to rely on this report, you will do so at your own risk.

We have satisfied ourselves, so far as possible, that the information presented is consistent with other information which was made available to us in the course of our work in accordance with our terms of engagement. We have not however sought to establish the reliability of the sources by reference to other evidence.

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Focus of this report

This report covers 14 countries worldwide that are amongst the leading providers of offshoring and/or outsourcing services. It focuses on the following matters:

1. What are the key laws or regulations that cover the application of employee security measures, whether during the recruitment process or on an ongoing basis?
2. What particular security screening measures are available to employers, taking into account legal, practical and cultural sensitivities?
3. What are the critical legal parameters that need to be taken into account when implementing security measures for employees

Executive summary

Background

This report covers 14 countries that are popular locations for offshoring or outsourcing work. These countries typically provide: access to English-language (or other major European language) skills; a low cost base relative to the domestic market of the organisation outsourcing or offshoring its operations; technical skills in areas such as information technology, computer sciences or engineering; a skilled workforce including a high proportion of graduates; and in some cases a large labour pool seeking employment. The combination of cost advantages and the availability of skills has led to a significant growth in the use of these offshore centres by large multinational businesses to the extent that it is now considered normal practice. In recent years small to medium-sized businesses have been outsourcing critical parts of their operations (manufacturing of products or volume administrative processes) to realise significant cost reductions and gain a competitive advantage.

Definition of 'outsourcing'

A practice used by different companies to reduce costs by transferring portions of work (and processes) to outside suppliers rather than completing it internally. Outsourcing is an effective cost-saving strategy when used properly. It is sometimes more affordable to purchase an item or service from companies with comparative advantages than it is to produce the item internally. Business process outsourcing (BPO) – for example, the examination of medical records (or the interpretation of scans or X-rays carried out in the home country, which is often undertaken in India), IT outsourcing and call centres – represents a significant element of outsourcing, as does the manufacturing of component parts for a product. Alternatively, businesses may decide to outsource book-keeping duties to independent accounting firms, as this might be cheaper than retaining an in-house accountant.

Offshoring and near-shoring

Both offshoring and near-shoring describe the transfer of a business process to another country, where that process is undertaken by a company or organisation within the same legal ownership structure, such as a subsidiary or joint venture of the parent organisation. In both cases, there is an inferred cost advantage in relocating a part of an organisation's work processes to a foreign jurisdiction.

'Near-shoring' is typically used to describe the process by which an organisation transfers business processes to a jurisdiction that is in close geographical proximity to the home country. For UK or Western European companies, near-shoring indicates the use of organisations located in the wider European area. This option offers certain advantages to these companies: organisations located within the European Economic Area (EEA) might offer a wider range of language skills that may not be readily available in more distant, offshore locations. Organisations within the European area may also be more closely aligned culturally with Western European organisations. As a result, they may have a better understanding of the business approach or needs of a Western European company than organisations located outside the European area. There may also be a geographical advantage to near-shoring operations, particularly in areas such as logistics that require handling of physical goods.

'Offshoring' typically involves the transfer of processes or operations to lower-cost jurisdictions that are more geographically distant from the domestic country. Countries covered in this report, including India, China, Malaysia and the Philippines in particular, are popular locations for offshoring operations. They generally offer a lower cost structure than near-shoring countries in the geographical European area (in part a consequence of a larger available labour pool). They also provide access to experienced skill sets. For example, for many years India has been a world leader in the provision of BPO and IT outsourcing operations within the technology and financial services sectors.

If a decision is made to outsource business processes to a third party the parent organisation should specify, subject to local laws and considerations, its exact requirements in respect to personnel security measures within the contractual agreement. Provision should also be made to permit the auditing of the third party's processes and procedures relating to personnel security for those employees engaged on the contract. Additionally, controls should be in place to prevent unauthorised sub-contracting of work and there should be a requirement for all breaches in personnel security in the offshore location to be reported to the UK management with immediate effect.

Employee security considerations

Regulatory and legal frameworks

The existence of laws or regulations that govern employment conditions in each country has a significant impact on the extent to which an employer may impose security measures, whether as part of the recruitment process, or on an ongoing basis.

There are a number of sources of relevant law within the EU. These include:

- the European Convention on Human Rights
- data protection legislation
- labour law or employment law
- right-to-work or equivalent immigration legislation
- health and safety legislation
- the Equal Pay Directive
- the Equal Treatment Directive
- the Race Directive
- electronic communications and telecommunications legislation
- legislation governing intellectual property rights and
- anti-money laundering legislation.

Within most EU States there is a certain level of consistency as a result of as a result of the legislative framework set out above, local variations in law and regulation remain on a country-by-country basis. Such variations include labour laws and criminal/penal laws that may restrict the ability of an employer to implement employee security or employee screening measures. For example, in Poland an employer's right to request information from a prospective employee is limited under the Labour Code; while in Bulgaria, Ireland, Romania and Slovakia, investigations involving criminal matters must be conducted by the police or a prosecutor or evidence gathered will not be admissible in court.

In general, data protection legislation places a duty on employers to ensure that any security measures imposed (in particular those that invade personal privacy, such as communication intercepts or surveillance) are proportionate to the threat faced. For example, an employer with specific grounds to suspect that a criminal activity is taking place may be able to implement more stringent security measures, such as covert monitoring of communications. The guiding principle of

proportionality, however, is not defined and ultimately will be at the discretion of the courts.

Countries in the EU each have a data protection commissioner (or equivalent) whose responsibility is to oversee the implementation of data protection legislation. Use of security measures likely to invade personal privacy (for example, use of visual surveillance in 'private' areas or monitoring communications without the consent or knowledge of an individual in situations where no serious matter such as a criminal offence is suspected) may lead to sanctions against the organisation by the data commissioner. Such measures may also breach constitutional or human rights legislation. Whilst an employer has a right to secure its assets, it is good practice to communicate security measures to employees to ensure that they understand and agree to the use of those measures. This practice has application both within and outside the EU. Certain countries within the Union, such as Ireland, also have strict intellectual property laws that supplement general data protection law. The existence of such laws in Ireland has supported the growth of the e-commerce sector in the country.

In countries outside the EU covered in this report, the laws concerning employment and employee security measures are generally less developed. For example, there is no specific data protection legislation in China or India (although some countries, such as India, Singapore and the Philippines, do have new and developing data protection provisions as well as certain intellectual property rights, which specifically protect certain categories of products or services, such as software licensing). Nonetheless, in these non-European countries there is also a generally accepted concept that measures should be proportionate to the threat (similar to the 'proportionality' concept in countries within the EU).

Countries outside the EU covered within this report all have an established labour law or employment code. These laws generally govern issues such as the right to work and the dismissal process. In general they do not favour either the employer or the employee. These codes may be specific as to conditions of employment, as is the case in South Africa, or open to wider interpretation, as is the case in China. Where laws are less closely defined, local legal advice should be sought on the application of security measures.

Practical and cultural considerations

In addition to the legal considerations outlined above, there are also local practical and cultural considerations. For example in China, although laws and regulations exist in relation to employment, their definitions are imprecise and open to subjective interpretation. Employees are prohibited from dealing in 'state secrets' although the obligation to determine what constitutes a 'state secret' is imposed on the citizen and not the state.

In countries such as China and India, frequently records (for example, residency information) are not held in a centralised or digital format. This presents practical difficulties for an employer seeking to implement pre-employment or ongoing personnel security measures, such as criminal records checks, or covert monitoring, for example. There may be few or no independent, reliable, third-party sources of information that would allow an employer to seek verification of information provided by a prospective employee during the recruitment process. In India, residency data may be difficult to verify because record keeping is decentralised, and often not stored in a searchable format. In some residential areas of major cities in India building does not follow strict and regimented patterns making address information erratic. In Morocco, for example, there is no developed, centralised, credit-reporting information. These practical issues may also impact on the timeframe for undertaking checks on prospective employees (for example, in India it is normal to visit the prospective employee's residence to verify address data provided).

Within the EU, although ongoing employee security measures are generally not restricted by law and regulation, not all measures outlined in this report are widely accepted practice, often for cultural reasons. For example, the use of reporting hotlines is not common practice in Poland, Romania, Bulgaria, the Czech Republic or Slovakia. In addition, there are ongoing issues of compatibility between US and EU law. The US Sarbanes-Oxley Act 2002 imposes duties on publicly held US companies and their EU-based affiliates to put in place procedures for confidential, anonymous reporting by employees of concerns over accounting or auditing matters. EU data protection legislation, meanwhile, protects personal data and stipulates that such reports must be confidential but not anonymous. Some countries' officials (such as Ireland's Data Protection Commissioner) have suggested that this issue may be overcome by ensuring that whistleblower reports are specific to issues but not to individuals. Financial regulators, such as the Central Bank of Ireland in 2011, have imposed EU-wide regulations requiring that approved individuals within international organisations headquartered in Ireland demonstrate fitness and probity. Under the Dodd-Frank Act 2010, the US government imposed global compliance requirements on financial institutions.

The use of pre-employment screening measures has become more prevalent within the countries covered in this report, predominantly as a result of the influence of Western institutions (principally those based in the United States or the United Kingdom) in which there is an established culture of pre-employment screening. Large international companies have often demanded the local implementation of employee security measures as part of group policies, and so there has emerged a standardisation of HR practice across international operations subject to local law and legislative provisions.

Recruitment of offshore staff

Pre-employment screening processes offshore should ideally be consistent with those undertaken in the UK (as set out by CPNI in *A good practice guide on pre-employment screening*). However, there will be some significant variations between countries in both the process of screening and the nature of the information returned. While such differences should not prevent a decision to offshore, they will need to be considered and addressed to maintain a good standard of personnel security across international operations.

Some of the issues organisations might encounter while attempting to assess potential local employees in an offshore location are:

- lack of official infrastructure, which can make obtaining comprehensive and centralised information difficult or impossible
- confusing and overly bureaucratic legal, governmental and administrative frameworks, which are difficult to understand and negotiate – this can make pre-employment screening checks particularly hard for UK-based human resource staff to obtain and interpret and
- in some countries, the potential ease with which official documents can be forged may also affect the extent to which an organisation can trust the information it receives from a potential employee and the number and extent of the checks required.

For UK companies and institutions considering offshoring, this guidance document offers information about what checks can reasonably be carried out in each of the 14 countries examined. The areas of focus centre around the core personnel security checks that are commonly carried out in the UK and each country profile details local variations and legislation affecting the processing of each check. The checks most often carried out are:

- identity checks

- checks into eligibility to work
- residency checks
- criminal record checks
- employment checks
- education checks and
- occupational health checks.

The procedures by which the checks listed above are carried out vary significantly between countries, as does the documentation that is typically requested and utilised to verify an individual's background and status.

Other employee security measures

Additional sources of information

In addition to the security measures set out in this report, many larger international employers routinely adopt additional measures (either during the recruitment period or as part of ongoing employment) that do not require the involvement of the employee concerned. This includes screening individual employee names against restricted-party lists (such as lists of entities subject to financial sanctions or embargoes) and undertaking other background checks, such as a review of press information, corporate affiliations, court records, bankruptcy or personal insolvency information, etc.

Screening against restricted-party lists

As a security measure, some employers (in particular larger, international organisations and those in the financial services industry) screen employee names against restricted-party lists to ensure that they do not employ an individual who is subject to financial or personal sanctions, or has been subject to enforcement action by a law enforcement authority or a regulatory body. The list below provides an overview of such sources of information. It should not be considered exhaustive.

Financial sanctions sources (major sources only)

- United States Treasury, Office of Foreign Assets Control – Specially Designated Nationals list (SDN list): http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fuzzy_logic.aspx
- HM Treasury, financial sanctions list: <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>
- United Nations Security Council Committees – UN sanctions: http://www.un.org/sc/committees/list_compend.shtml

Such lists may be checked individually or through commercial compliance tools that consolidate all of the principal international sanctions lists and permit you to run searches across them all simultaneously.

Other forms of background check

Depending on the role and responsibilities of a prospective employee, certain employers (in particular those organisations subject to regulatory oversight, or organisations that deal with sensitive data) undertake an additional range of checks into prospective employees. Such checks will depend on the level of information available in each particular jurisdiction and whether the check is proportionate to the role. These include:

- reviewing corporate records to ascertain whether an individual holds any corporate appointments or directorships, current or resigned – such a check may include searches to ascertain whether the individual has been disqualified or disbarred from holding office
- searching for any bankruptcy or personal insolvency information (where such information is searchable and available in the public domain)
- media checks involving open source information (such as internet, newspapers and publications) to determine whether an individual has been engaged in any activities that could be considered criminal, fraudulent or that could be judged as conflicting with the interests of the business
- professional qualifications that are specifically required in order to perform a job role (e.g. accountancy qualifications for accountants or legal qualifications for lawyers) should be verified directly with the awarding body or, if a licence is required, directly with the industry regulator and
- formal criminal record checks (in higher-risk roles) that obtain a certificate of good conduct/ certificate of no conviction/criminal record extract from the local police force, or Ministry of Justice or of the Interior.

The final process listed above is usually driven by the individual and employers must obtain that person's consent to carry these checks out. In many European countries employers have the right to request such certificates, but equally individuals have the right to refuse to provide them for employment purposes.

Ongoing personnel security offshore

Maintaining a high standard of ongoing personnel security measures and ensuring that employees are well treated will raise morale and may also increase the psychological commitment of local staff to the organisation, reducing the likelihood of insider activity. This may be particularly so in countries that do not have any trade unions to represent employee groups or those with poor human rights records.

All personnel-related security measures should be directly proportionate to the threat faced, as determined by a personnel security risk assessment (see CPNI's *Personnel Security Risk Assessment: A Guide*) for further information. This is equally important in an offshore environment and organisations should remember that, just because a particular security measure is legally permissible in a given country, this does not necessarily mean that it will be useful or proportionate.

Access controls

None of the 14 countries examined within the guidance have any apparent legal restriction on controlling physical access to buildings or zones, other than where biometric data is restricted by a provision within a data protection law. Physical screening is permitted in all countries, but is often restricted to same-gender searching protocols and is not widely used.

In the UK, CPNI recommends using role-based access, an approach that determines the physical and informational access an employee will have by reference to their job role. These access rights should be regularly reviewed and automatically re-evaluated when an employee changes jobs.

The same approach is recommended in offshore locations, particularly where there is potentially less assurance regarding an employee's background and integrity, owing to an absence of verifiable information. In addition, where staff are transferred or promoted within the offshore location or between the offshore base and the UK, the risk assessment should be reviewed and amended as required.

Protection of data

In the UK, organisations have a duty to ensure, where appropriate, that employees are aware of their obligations regarding the protection of sensitive or valuable information; for example, to ensure compliance with their respective in-country data protection law. Although there may be variations between the laws in different locations, the same principles apply offshore. Access should be limited by reference to an employee's role, and where a high level of access is needed, additional safeguards may be required to limit that employee's ability to disclose, print or copy particular information. The following measures may be considered:

- requiring staff to sign a confidentiality agreement as part of their employment contract – this should specify that corporate information must not be disclosed to anyone outside the organisation and clearly outline the consequence of any breach of the agreement
- restricting employee access to printers, photocopiers, data storage devices and email, particularly where sensitive data is involved and
- searching employees (either all employees or at random) as they enter or exit the building – this can act as a deterrent and contribute to the detection of any unauthorised items and/or the removal of assets or information.

Employee monitoring

The subject of employee monitoring can be a sensitive one, with a pervasive idea that we do not like the thought of someone continually watching over us. Consequently, if the rationale for adopting such measures is not well communicated, they may undermine staff trust and morale. However, most monitoring systems do not actually focus on a single individual, but rather take in a large volume of data across a wide group of employees, enabling security staff to spot patterns that appear anomalous, compared to a norm. This kind of monitoring is generally more palatable.

In many countries, there is legislation in place regarding the use (or prohibition) of overt and covert monitoring systems. It is, of course, important to comply with local legislation and legal advice should be sought before implementing any new measure to monitor employees, particularly monitoring telephone communications or covert IT monitoring.

In the UK, public authorities covered by the Human Rights Act 1998 must ensure that any interference with privacy is necessary and proportionate for a legitimate purpose (listed in the Act) and accords with the relevant law (for example, the Regulation of Investigatory Powers Act 2000).

Reporting hotlines

Very few countries prohibit the use of reporting hotlines, although their deployment is not common practice in Poland, Romania, Bulgaria, the Czech Republic or Slovakia, if they are used at all. This may arise from cultural sensitivities or perhaps from negative associations attaching to reporting hotlines.

There is also an ongoing issue of compatibility between the US Sarbanes-Oxley Act 2002, which requires organisations to provide an anonymous reporting mechanism for accounting or auditing matters, and EU data protection legislation, which stipulates that a hotline must be confidential but not anonymous. To overcome this dichotomy, some countries (for example, Ireland) have suggested that a whistleblower's report should be specific to an issue but not an individual.

Investigative techniques available offshore

Maintaining the ability to investigate and resolve security-related concerns about an individual or incident in an offshore location is a key aspect of personnel security. However in some offshore locations the legislation surrounding investigation is vague and it may be unclear whether a particular investigative activity is permitted. In such circumstances an organisation should consult a legal expert and proceed with caution.

It may be useful to have a security (and possibly HR) capability *in situ*, as it can be very difficult to oversee security and disciplinary procedures remotely. However, it may be necessary for at least some security and HR employees to be drawn from the local community. Where this is the case, the parent organisation should ensure that such individuals are subject to the same level of pre-employment screening as their UK counterparts. Where this is not possible, additional, ongoing security measures may be required, depending on an individual's responsibility and access.

Prevention of insider activity is always preferable to its cure and an investigation is likely to be more resource-intensive than most other personnel security measures. For this reason, an investigation should be viewed as a necessary means to resolving unpreventable insider incidents, rather than as a preventative measure in its own right (although a good investigative capability will also act to deter insider behaviour).

The purpose of an investigation will inform and may dictate the course of events (for example, the process of collecting evidence for a criminal prosecution case involving a law enforcement agency will differ from that for an internal disciplinary event). Investigative activities, as outlined on the following pages, may be undertaken by the organisation, by a private investigator or by local police authorities, depending on the location and circumstances.

Licensed investigators

Most countries have some form of legislation in place regulating the work of private investigators, but some do not, owing to the local cultural perceptions of licensed investigators. For an organisation, the capability to conduct its own investigations can be extremely useful, particularly where there are finite resources available to the local police. However, this process can be resource-intensive and the powers of such investigations may be limited. Moreover, serious incidents must be referred to the local or state authorities.

In China, legislation concerning the private investigations industry continues to develop and activities that are currently permissible might not be under the new laws. Companies conducting their own investigations should be alert to these potential changes and consult local legal experts to ensure that their investigative endeavours are compliant.

Surveillance

Some forms of surveillance do not focus on one individual but look across a number of employees. For example, some CCTV systems store data that can be scrutinised retrospectively if an insider incident later comes to light. In Romania, only the state authorities can perform surveillance of any type, regardless of the suspected or alleged offence, while in China, the Czech Republic, Ireland and the Philippines, the use of different forms of surveillance is restricted by reference to the severity of the incident and the intrusiveness of the surveillance.

Most countries do not prohibit surveillance of transactions – for example, records of telephone call, email logs and financial transaction data – although some restrict this to information obtained directly from company premises or systems.

Intercepting communications

Most countries regulate, restrict or prohibit the use of interception as an investigative tool, with the exception of Singapore where there are currently no legal restrictions. In India and Poland, employees may only be searched for company systems, equipment or property. In China ‘bugging devices’ are illegal, but it is unclear whether other forms of intercept, such as telephone call monitoring, are permitted.

Interception conducted from the UK of the communications of employees abroad may be regulated by the Regulation of Investigatory Powers Act 2000 and, if not properly authorised, could constitute a criminal offence under that Act. If in doubt, legal advice on the specific situation should be sought.

Interview

None of the countries examined in the guidance indicate that an interview is not a permitted method of investigation, although in some countries such as Romania an interview conducted internally by an organisation could not be used as evidence in a criminal case.

Nevertheless, an informal interview (conducted in accordance with the local legal framework, company policy, human rights and health and safety legislation) can be an extremely cost-effective way of determining whether an individual merits closer scrutiny or if there is an innocent explanation of the circumstances that prompted the initial suspicion.

Search/seizure

Neither Ireland nor Romania permits search or seizure by any entity other than the police, and in the other countries examined the procedure is restricted or regulated. Even the most permissive countries limit such activity to searches for company equipment, systems and property.

Any employee subject to such a procedure is likely to be alienated by the experience and it is important that it is only conducted at a stage of an investigation when it becomes clearly necessary. If subjected sooner than this, there is a danger that such an individual may become, or become more, disaffected with the organisation and then be more likely to engage in insider activity.

Involving the police in an investigation

The expectation of whether and when local police should be involved in an insider investigation varies between countries and depends on both police resources *in situ* and the nature of the incident. For example, in Poland any insider incident occurring within the public sector must be reported to the police as a matter of course and at the earliest opportunity, while private industry is under no obligation to report any insider incident. In contrast, for an organisation in Singapore, one of the main considerations is whether there is enough evidence for the police to prosecute, and in Ireland the police must be involved from the outset if a criminal prosecution is the desired outcome.

Generally, the police only need to be informed where it is clear that a criminal offence has been committed or where the matter is sufficiently serious to require their involvement. However, in many instances it may be more appropriate for an organisation to investigate insiders internally, without involving the police. Whatever course of action is undertaken, it is important to ensure that the response complies with the law within the country concerned, taking local legal advice where necessary.

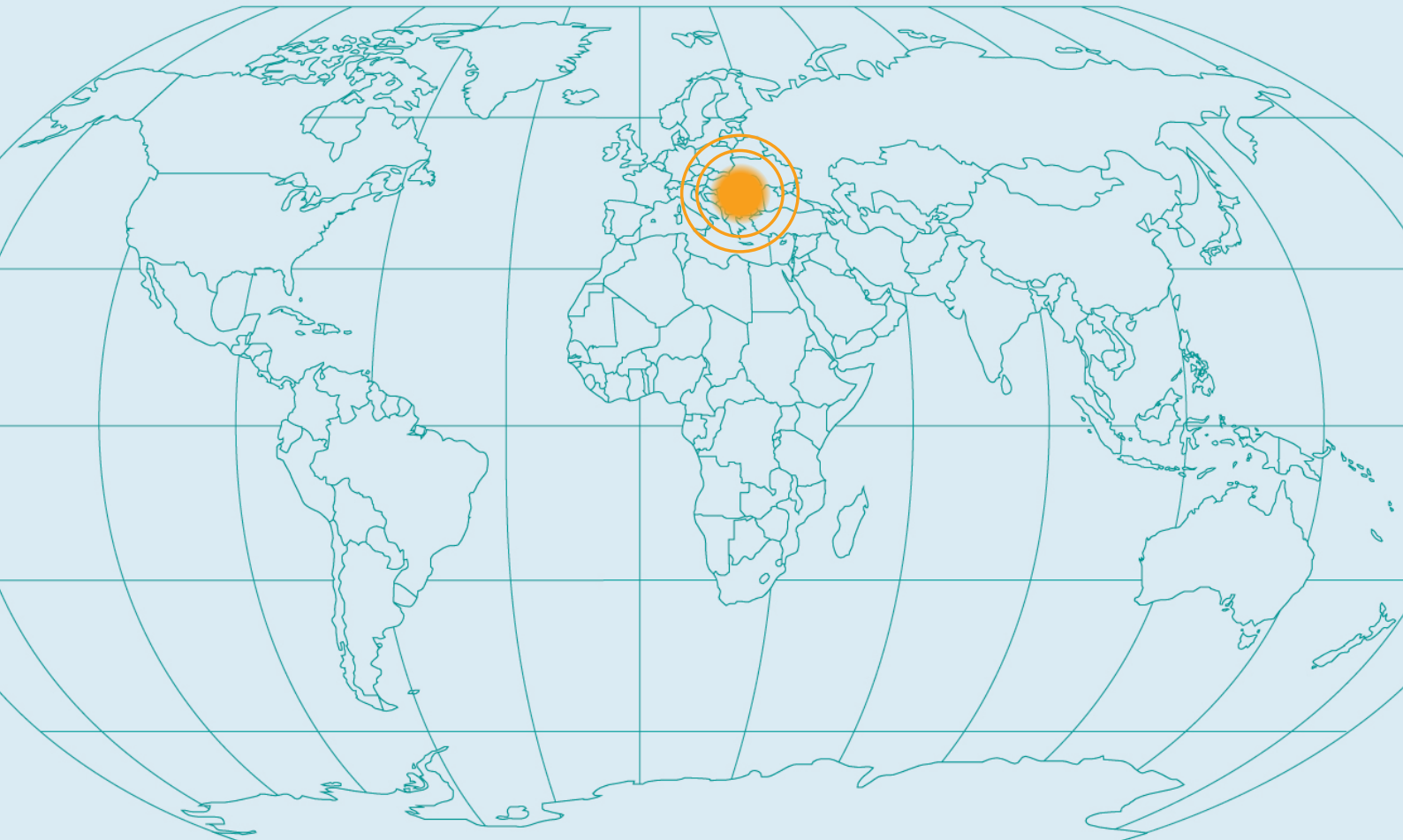
CPNI

Centre for the Protection
of National Infrastructure

SECURITY **WATCHDOG**
Part of Capita plc

Bulgaria

Personnel Security in Offshore Centres



Bulgaria

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1

Introduction

Bulgaria has become a popular location in Europe for outsourced operations. This arises from a combination of factors: its labour costs are amongst the lowest within the European Union (EU) and compare favourably with other significant offshore centres such as India; it benefits from a highly educated workforce, with a large pool of graduates. English is widely spoken and the country benefits from close cultural ties with Western Europe. Bulgaria has particular skills in areas such as electronics, computer sciences and engineering. Outsourcing companies in the country are regularly involved in providing IT outsourcing and software services. Bulgaria's membership of the EU also affords greater protection to employers and employees, for example in the area of data protection.

Employment measures in Bulgaria are governed principally by the Labour Code. The Code sets down the rights and obligations of employees and employers. The purpose of the Code is to establish a basic minimum level of requirements. This includes regulations on measures governing health and safety in the workplace.

Pre-employment security screening measures are generally available to employers in Bulgaria, and it is common practice (particularly for more senior positions or posts involving access to sensitive materials) to carry out a range of background checks. These measures are subject to personal data protection legislation and anti-discrimination legislation. An individual must generally provide consent to disclosure of personal information, such as employment references or credit checks. Data protection legislation also applies to the conduct of ongoing employee security measures. Any measures undertaken by an employer should pay due regard to data protection legislation which affords protection to personal rights and privacy. All pre-employment security screening measures should be reasonable, proportionate to the job role and carried out with the consent of the individual. As a member of the EU, Bulgaria has also enacted human rights legislation. Article 8 of the European Convention on Human Rights guarantees an individual's right to respect for private and family life. Any security measures undertaken (particularly those involving possible intrusion into private life, or private 'areas') should take into account such legislation.

2	Personnel security measures during recruitment	
2.1	Culture of screening	<p>Pre-employment security screening measures may be undertaken in Bulgaria, subject to a number of laws and regulations. In particular, this includes anti-discrimination law, personal data protection law and the Labour Code. Where pre-employment screening is performed, the level of review is generally commensurate with the industry in which they are working and the proposed role and responsibilities of the applicant at the employer’s organisation. Both the government sector and several other sectors, such as banking and financial institutions, have established pre-employment security screening procedures. In addition, it is usual for international organisations with operations in Bulgaria to apply pre-employment security screening as part of a corporate security process that applies to all international operations. Such screening would seek to identify discrepancies in the background of an individual, such as education, qualifications or references.</p> <p>In Bulgaria, the employer is responsible for ensuring that an individual has the right to work in the country.</p>
2.2	Major laws and regulations applying to pre-employment screening	<p>The major laws and regulations that apply to pre-employment screening in Bulgaria are as follows:</p> <ul style="list-style-type: none"> • The Labour Code, as amended, is the major legislative item that governs all aspects of employment in Bulgaria and the relationship between the employer and the employee. In particular, the Code regulates the following aspects of employment: <ul style="list-style-type: none"> – the rights and obligations of the employee and the employer under the employment contract – working hours, holidays and absence periods – protection accorded to certain categories of employees – the governance of employment contracts including conclusion of the contract, amendment and termination – employment discipline and – the compensation of an employee. • The Protection Against Discrimination Act prohibits any direct or indirect discrimination on grounds of gender, race, nationality, ethnicity, human genome, citizenship, origin, religion or belief, education, convictions, political affiliation, personal or social status, disability, age, sexual orientation, marital status, property status or on any other grounds established by law or by an international treaty to which Bulgaria is a party. An employer cannot request such information as part of the pre-employment screening process, except in extraordinary circumstances. • The Personal Data Protection Act (derived from the European Data Directive 95/46) ensures the protection of individuals against unauthorised processing of personal data relating to them, in the process of free movement of data. Under the Act, ‘personal data’ means any information relating to an individual who is identified or identifiable, directly or indirectly, by reference to an identification number or to one or more specific features. Personal data may be processed only so long as at least one of the following conditions is met:

- 1 processing is necessary in order to comply with an obligation imposed on the personal data administrator by a piece of legislation;
- 2 the individual to whom such data relate has given his or her explicit consent;
- 3 processing is necessary for the fulfilment of obligations under a contract to which the individual to whom such data relate is party, as well as for any activities initiated by the same individual prior to the conclusion of such a contract;
- 4 processing is necessary to protect the life and health of the individual to whom such data relate;
- 5 processing is necessary for the performance of a task carried out in the public interest;
- 6 processing is necessary for the exercise of an official authority vested by law in the administrator or in a third party to whom the data are disclosed; or
- 7 processing is necessary to realise the legitimate interests of the personal data administrator or a third party to whom the data are disclosed, except where such interests are overridden by the interests of the individual to whom such data relate.

- The **Bulgarian Penal Procedure Code** (last amended in 2014) governs the rehabilitation of individuals. Under the Code, the rehabilitation shall remove the conviction from the record and shall revoke for the future the consequences ascribed by laws to the conviction itself. Once the conviction is 'spent', the rehabilitated person does not have to reveal its existence in most circumstances. However, for certain professions (for example, in the Ministry of Internal Affairs) individuals are required to detail all convictions and criminal charges, whether spent or unspent.
- Caution should be taken in the disclosure of information in case it is restricted under law. Article 416 of the proposed 2014 changes to the Penal Procedure Code carries a one-year jail term for unlawful disclosure.
- The European Convention for the Protection of Human Rights and Fundamental Freedoms has direct application in Bulgarian law. Beside the Constitution of Bulgaria, it is the main source of human rights protection in the country. The Convention Articles most relevant in relation to Bulgarian law are:
 - Article 4: prohibiting forced labour
 - Article 6: right to a fair trial
 - Article 8: right to respect for private and family life
 - Article 9: freedom of thought, conscience or religion
 - Article 10: freedom of expression
 - Article 11: right to free assembly or association and
 - Article 14: freedom from discrimination.

Article 8 is particularly relevant to employment situations.

It is relatively rare in Bulgaria for cases to be brought under the Convention as provisions elsewhere in employment law are more relevant. In particular, there is the Protection Against Discrimination Act (see above).

3	Pre-employment checks	
3.1	Identity check	<p>Undertaking identity checks provokes no sensitivities in Bulgaria</p> <p>Official Bulgarian identity documents are personal identity card, passport or drivers' licence.</p> <p>A temporary passport, a border pass or a temporary passport for definitive departure from the Republic of Bulgaria may also act as official documents to prove that an individual is a Bulgarian national.</p> <p>Marriage, birth or adoption certificates and tax notifications offer a lower level of identity verification and are not recognised as identity documents.</p> <p>The validity of a Bulgarian ID card, driving licence, international passport or sailor's passport can be checked on the website of the Ministry of Internal Affairs by entering the document number at the following website:</p> <p>http://validni.mvr.bg/nbds2/web2.nsf/fEnVerification?OpenForm</p> <p>The national ID card conforms to EU-wide standards.</p>
3.2	Checks on eligibility to work	<p>This does not apply to Bulgarian nationals, nor to citizens of the EU, who have a right to work in Bulgaria, without restriction.</p> <p>Generally, foreigners (as defined by the Foreign Nationals Act) may work in Bulgaria only after obtaining a work permit. An employer should apply for a work permit on behalf of a prospective employee. Work permits are issued by the Employment Agency. The work permit carries specific conditions and is issued for a maximum duration of one year. As a mandatory prerequisite a foreigner must be granted a long-stay visa to qualify for a work permit.</p> <p>Certain categories of foreigner may work in Bulgaria without a work permit:</p> <ul style="list-style-type: none"> • managers of companies, or branches of foreign legal entities • members of the Managing Board or Board of Directors of local companies who are not employed on a labour contract; • trade representatives of representative offices of foreign companies registered at the Bulgarian Chamber of Commerce and Industry and • foreigners with a right of permanent residence in Bulgaria. <p>The legal status of foreigners in Bulgaria is covered by the Constitution of the Republic of Bulgaria, the Foreign Nationals Act (effective 1998), the Regulation on the Application of the Foreign Nationals Act, the Ordinance on Issuing Visas and the Ordinance on Issuance of Work Permits.</p> <p>Employers must also register foreign workers at the National Revenue Authority within three days of commencement of employment, regardless of whether a work permit is required or not.</p> <p>Further information regarding work permits is available from the National Office of Employment of the Labour and Social Security Policy Ministry.</p>

3.3	Residency checks	<p>This check is often included as part of the identity check, since the individual's current address should be on the reverse of their national ID card.</p> <p>Alternatively, the employee may present to the employer a certificate for permanent and current address (local council address card), issued by the municipality in which he/she is a resident. If an employer wishes to validate residency data, it should request the employee to present such a certificate.</p>
3.4	Criminal record checks	<p>Name of certificate</p> <p>Conviction Status Certificate (Свидетелство за съдимост)</p> <p>Department that holds records</p> <p>Central Office of Criminal Records and all Regional Courts in Bulgaria</p> <p>Where to apply within country</p> <p>Individuals born outside Bulgaria or with an unknown place of birth apply at:</p> <p>Central Office of Criminal Records, Ministry of Justice, 5 Aksakov Street, 1040 Sofia, Bulgaria.</p> <p>Telephone: +359 (0) 2 92 37 355 Website: www.justice.government.bg/44/ Email: pr@justice.government.bg or priemna@justice.government.bg</p> <p>Individuals born in Bulgaria apply at local Criminal Records Offices of the Regional Courts. A list of these can be found at: www.vss.justice.bg/bg/start.htm</p> <p>How to apply within country</p> <p>In person</p> <p>To a local Criminal Records Office of the Regional Courts or the Central Office of Criminal Records (see contact details above).</p> <p>Together with the individual's:</p> <ul style="list-style-type: none"> • ID card • original birth certificate and • proof of payment, <p>third parties should present a power of attorney, authorising them to obtain the certificate.</p> <p>Online</p> <p>Applications are made through the Ministry of Justice website at https://cs.mjs.bg/</p> <p>This route may only be used by individuals who have no convictions or administrative sanctions imposed.</p>

		<p>Who can apply</p> <p>Individuals or third parties (with consent).</p> <p>Cost, payment and turnaround</p> <p>Cost</p> <ul style="list-style-type: none"> • BGL 3 <p>Payment</p> <ul style="list-style-type: none"> • Central Office of Criminal Records: <ul style="list-style-type: none"> – bank transfer to: <ul style="list-style-type: none"> – Bank account of the Central Office of Criminal Records – IBAN: BG09BNBG96613000173701 – BIC: BNBGBGSD • Criminal Records Offices of the Regional Courts: <ul style="list-style-type: none"> – bank transfer to the bank account of the respective Regional Court (contact the court for details) <p>Turnaround</p> <p>The certificate will be issued on the same day or no later than three working days after the application has been submitted.</p> <p>Legislation</p> <ul style="list-style-type: none"> • Penal Procedure Code of Bulgaria • Law on Electronic Document and Electronic Signature • Law on Protection of Personal Data <p>Further information can be obtained from the CPNI guidance on Overseas Criminal Record Checks which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>
3.5	Education checks	<p>Education checks are often required by employers to establish that a prospective employee has attended the educational establishments claimed.</p> <p>Typical information provided is dates for joining and leaving the educational institution (school, college or university), subject of study, courses (college, university), degree and final mark. In many cases, depending on the educational institution and its interpretation of the data protection legislation, this information is confirmed only and not volunteered.</p> <p>The Rector of the University (the President of the College) may refuse at his/her own discretion to give any information. Furthermore, often questions regarding the character of an individual will not be answered by educational institutions in writing, although in some cases a character reference may be obtained verbally from a tutor or professor who knows the individual.</p> <p>Information covered by the Protection Against Discrimination Act cannot be obtained, except in circumstances where it is not considered as discrimination.</p>

		<p>Applications for references must typically be made in writing and provide all known information – e.g. full name, date of birth, subject of study – and should explain the reason for the request. However, whether any information will be disclosed or not depends on the discretion of the Rector of the University (the President of the College). Consent of the individual is generally not required although obtaining this should be encouraged.</p> <p>Typically, results of education checks must be provided on headed notepaper. This ensures that the issuing institution carries a certain liability for the correctness and reliability of the data.</p> <p>Where the educational establishment is not well known, it may be necessary to undertake additional checks to verify the data’s authenticity. In particular, employers should be alert to the risk of fake establishments and/or fake qualifications issued by such establishments.</p>
3.6	<p>Qualification checks</p>	<p>Verification of qualifications (academic or professional) is used as part of the pre- employment screening process in Bulgaria.</p> <p>Typical information provided is dates for joining and leaving the educational institution or professional body, membership status (professional body) and status and type of qualification. In many cases, all known information has to be provided. The institution will usually confirm information, although it might not volunteer any data.</p> <p>Generally, questions regarding the character of an individual will not be answered by educational institutions in writing, although in some cases a character reference might be obtained verbally from a tutor or professor who knows the individual.</p> <p>Information covered by the Protection Against Discrimination Act cannot be obtained, except in circumstances where it is not considered as discriminatory.</p> <p>Application is made directly to the educational establishment or professional body concerned. Most educational establishments have standard processes for dealing with reference enquiries. Consent of the individual is generally required and recommended. Most professional bodies issue directories of members, so the accuracy of claimed status can be verified directly with the professional body. The information may sometimes be available online.</p> <p>Consent of the individual is generally required except in circumstances where the information is publicly available.</p> <p>Fake documentation is widespread and it is regularly reported that a proportion of employment candidates lie or exaggerate about qualifications. For example, attendance at an educational establishment does not mean the individual graduated from that establishment. It is also important to verify that an individual is an active member of a professional body and has not left, nor been ejected from membership.</p>

3.7	Employment references	<p>Prospective employers should ask to see a potential employee’s Labour Book as a means of validating their employment history.</p> <p>An individual’s Labour Book will also contain their social security number (Uniform Civil Number).</p> <p>Previous employers might provide references upon direct request. These might confirm basic information such as dates of employment, positions held and reason for leaving. They will rarely include character references or personal comment.</p> <p>Many employers may refuse to provide character references or comments on performance, written or verbal. Also, most employers will not provide information on salaries, sickness record or parental leave.</p> <p>Application is generally made in writing to the relevant employer.</p> <p>An employee must provide his/her consent to the obtaining of such information, in accordance with data protection legislation.</p>
3.8	Financial/ credit checks	<p>Such checks are generally used only for more senior roles or those that involve access to financial systems or controls (in particular in the banking and government sector). They are not commonly carried out outside the government or financial sectors.</p> <p>Financial or credit checks may be undertaken during the pre-employment screening stage, or on an ongoing basis more regularly where suspicions or concerns arise.</p> <p>In Bulgaria credit information relating to individuals and organisations is held in the Central Credit Register at the Bulgarian National Bank. An individual may verify his or her own credit record directly with the Bank. The Central Credit Register may also be accessed by banks in Bulgaria. A third party may access information on an individual, with the express, prior, written consent of the individual. The Bulgarian National Bank will provide credit information within seven days of submission of a written application, presentation of an ID card or a copy of an ID card certified by a notary public for the relevant individual. A fee is also payable.</p> <p>For further details see Ordinance No. 22 of the Central Credit Register</p>
3.9	Substance abuse screening	<p>The Labour Code explicitly sets out provisions banning employees from using alcohol or drugs in the workplace. An employer is free to establish its own rules and procedures for ensuring compliance with the Code.</p> <p>On signing an employment contract, the employee should be made aware of such provisions.</p> <p>In practice, screening for substance abuse is not widespread and it is typically used only in specific cases (such as for drivers of public transport vehicles). Where it is used, it may be part of ongoing security: either random screening or where there is suspicion of substance abuse.</p>

		<p>Substance abuse screening is likely to be a sensitive topic and normally would be applied only in specific situations (e.g. the prospective employee presents a heightened level of risk to the employer because of prospective position/access rights, etc.)</p> <p>Explicit consent of the individual would always be required.</p>
3.10	Occupational health checks	<p>Under the Labour Code, all employees must undergo periodic health check-ups. The frequency of these checks depends on the category of employment and the age of the employee.</p> <p>The guidelines are governed by the Ministry of Health. An employer is legally bound to meet the costs of such check-ups.</p> <p>Ordinance 4 of the Labour Code sets out the documents that must be presented as a condition of signing an employment contract. This includes a medical examination document.</p> <p>Although not specifically stipulated under the Labour Code, it is common practice for employers to require ongoing, regular health checks.</p>
4	Personnel security measures during employment	
4.1	Legal requirements	<p>The following legislation applies to ongoing personnel security measures in Bulgaria:</p> <ul style="list-style-type: none"> • The European Convention for the Protection of Human Rights and Fundamental Freedoms. <p>Organisations should bear in mind the importance of respecting employees' Article 8 right to private and family life. Organisations conducting an investigation which may involve the collection of information relating to an employee's private life should ensure that any resultant infringement of the right to privacy can be justified. This means that the amount and extent of all evidence collected should be both necessary and proportionate in the context of the type of investigation being carried out and the nature of the incident or suspicion.</p> <ul style="list-style-type: none"> • The Personal Data Protection Act (DPA) (see Section 2.2). • The Private Security Business Act regulates the following types of activity: <ol style="list-style-type: none"> 1 personal protection of individuals; 2 protection of the property of individuals or legal entities, which represents activity for physical protection of the property against illegal encroachment – this protection may also include the introduction of a scheme for admission to the facilities; 3 guarding events, for which it provides a set of measures directed at ensuring the undisturbed and unimpeded holding of mass events or activities of a short-term nature;

- 4 guarding valuable consignments and goods – protecting money, securities, precious metals, works of art and other valuables the transportation of which must be carried out under armed guard, using specially equipped transport, reliable communication and other means of technical and auxiliary protection; and
- 5 self-protection, which means an activity carried out by employees of the legal entity, assigned to separate structural units for guarding employees, facilities, events, property, valuable consignments and goods. The self-protection units may not be used in any way to guard persons, facilities and property other than those of the self-protected legal entity.

All of activities 1–5 above may also be carried out through technical security systems and auxiliary devices. Protection with the help of technical security systems means surveillance or control of the guarded facilities by technical means and checking the obtained signals.

- Under the Labour Code, employees who believe they have been dismissed unfairly can complain to a tribunal.
- The **Act on Health and Safety No. 124/1997** (as amended) regulates health and safety legislation in the workplace. It imposes duties on both the employer and the employee. In addition, the Labour Code sets down strict obligations on an employer to provide a safe and healthy working environment. As part of this, an employer must undertake an assessment of health and safety risks, to be performed by an independent, specialised company. It must develop a programme for monitoring health and safety conditions, based on an annual risk assessment. It must also provide protective measures and training to ensure the health and safety of employees.

There are two main trade union confederations in Bulgaria: the Confederation of Independent Trade Unions of Bulgaria (KNSB or CITUB) and Podkrepa. A third trade union confederation, Promyana, is much smaller than the largest two. Trade union activity is regulated under the Labour Code as well as numerous other legislative acts and regulations such as the Settlement of Collective Labour Disputes Act and the Act on Health and Safety.

Under the Bulgarian Labour Code, employees are entitled to freely form trade unions, with no prior permission required, and to join and leave them on a voluntary basis. In general, trade unions are able to represent employees' interests before State bodies and employers in respect to issues of industrial and social security relations and living standards, and protect them through collective bargaining, participation in tripartite cooperation, organisation of strikes and other actions permissible within the law.

Trade unions are entitled, within the limits of the law, to autonomously adopt their statutes and rules, to freely elect their bodies and representatives, to organise their leadership, as well as to adopt programmes of action. Of importance are the representative trade unions at national level. In order to become a representative trade union, an organisation should meet the following criteria:

		<ul style="list-style-type: none"> • membership of at least 50,000 individuals • comprising at least 50 organisations with no fewer than five members each in more than one-third of industries designated by the Council of Ministers in accordance with the National Classification of Economic Activities • comprising local bodies in more than half of the municipalities in the country and a national governing body and • the legal person must be registered as a non-profit organisation. <p>Recognition of the representative trade unions is granted by the Council of Ministers.</p>
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	The employer may be protected by intellectual property rights (under libel, slander and trademark law), and rights imposed under the employment contract. Legal action for breach of contract may restrain an employee from dealing in client-confidential information; however it is unlikely to deter more serious offences without the imposition of other controls (such as physical access controls, or monitoring controls as described below).
4.4	Local legislation that specifically governs the rights of the employee	As detailed above, there is legislation that governs the rights of an employee (and third parties). This may restrict the level of self-protection permissible. However, under the DPA, the gathering and processing of personal data necessary to meet the legitimate interests of the personal data administrator (the employer) is permissible, if such interests are not overridden by the interests of the individual (the employee) to whom such data relate.
4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	Individuals may bring claims against their employer under the legislation set out above.
4.6	What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?	<p>A claim for unfair dismissal may be brought under the Labour Code under one of the explicitly specified preconditions therein. Furthermore, under the DPA, a complaint for breach of an employee's rights may be submitted by the injured party to the Commission for Protection of Personal Data, which may impose requirements and sanctions on the employer. Beside the complaint before the Commission, under the DPA the employee whose rights have been breached is entitled to file a claim before the administrative court.</p> <p>An employee may be dismissed only on the grounds explicitly provided for by the Labour Code. Dismissal may or may not require advance notice, according to the conditions of the Labour Code. Where notice is required, the period may vary from 30 days to 3 months.</p>

		<p>Where an employee is subject to disciplinary proceedings there is a three-step disciplinary, dismissal and grievance process that must be followed in each case. Failure by the employer to follow the statutory procedures prior to dismissal will render that dismissal automatically unfair. The employee is entitled to claim to be restored to their position and to claim compensation for unfair dismissal against the employer.</p> <p>The three main stages of the disciplinary process are:</p> <ul style="list-style-type: none"> • notification to the employee • written explanations by the employee or hearing of the employee at a meeting with the employer and • a written order for disciplinary dismissal giving the reasons for the dismissal, which should be handed to the employee for his/her signature, setting out the appeals process before the court.
4.7	Availability of security measures	<p>Restriction of access to the premises</p> <p>No specific restrictions exist.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>No specific restrictions exist.</p> <p>Physical screening (on entry/exit)</p> <p>No specific restrictions exist.</p> <p>Prohibition of removal of data from the premises (hard-copy)</p> <p>The DPA governs protection of personal data. Removal of data from the premises or from secure systems may constitute a breach of the DPA.</p> <p>Prohibition of removal of data from the premises (electronic)</p> <p>See above.</p> <p>Visual surveillance (CCTV or other cameras), either overt or covert</p> <p>The Private Security Business Act governs the use of surveillance and physical control measures in guarded facilities and the review of information obtained.</p> <p>Overt monitoring of access to IT and other equipment</p> <p>Where monitoring involves the collection of personal data, the DPA requires that such data are collected lawfully and processed in a fair and proper way.</p> <p>Covert monitoring of access to IT and other equipment</p> <p>See above.</p> <p>Reporting hotlines (anonymous)</p> <p>Personal data must be handled in accordance with the DPA.</p> <p>Reporting hotlines (confidential)</p> <p>Personal data must be handled in accordance with the DPA.</p>

		<p>Use of alerts/automated warning systems to identify unusual employee behaviour (out-of-hours activities, duplicate payments)</p> <p>The use of automated warning systems is not specifically regulated by law or regulation. The employer should assess the need for such a system based on the overriding requirements under the data protection legislation to demonstrate a proportionate response to risks.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>Where monitoring involves the collection of personal data, the DPA requires that such data are collected lawfully and processed in a fair and proper way.</p>
4.8	Formal investigations	<p>Is there a licensing regime covering investigators?</p> <p>There is no specific licensing regime in Bulgaria that covers investigators.</p> <p>Physical surveillance (overt or covert)</p> <p>Physical surveillance is covered by the Constitution of the Republic of Bulgaria, the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Private Security Business Act.</p> <p>The Private Security Business Act does not provide detail about the application of physical surveillance.</p> <p>The law does not distinguish overt and covert surveillance and nor does it include the concept of proportionality.</p> <p>Electronic surveillance (e.g. tracking devices)</p> <p>This is subject to the laws set out above (physical surveillance).</p> <p>Visual and communication surveillance (using cameras, video or CCTV)</p> <p>Visual surveillance is covered by the Constitution of the Republic of Bulgaria, the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Private Security Business Act. Where visual surveillance is used on employers' premises, it is good practice for the employer to communicate the use of surveillance cameras by warning notices. There is no requirement to identify the location of the devices. The video recordings obtained should be destroyed not later than 30 days after they have been made, and a written record of their destruction should be made, except in cases where they contain data on a committed violation of public order or a crime, in which case the recordings should be submitted to the law enforcement authorities. Therefore, if the matter does not relate to a criminal investigation and is not passed to law enforcement authorities, the recording should be destroyed within 30 days. It is good practice to maintain a written protocol.</p>

Communication intercept (including oral, written and electronic communication including bugging devices)

The use of communication intercept is subject to the Constitution of the Republic of Bulgaria, the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Private Security Business Act.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

Use of computer or database surveillance is subject to the Constitution of the Republic of Bulgaria, the European Convention for the Protection of Human Rights and Fundamental Freedoms (in particular the duty not to invade personal space, which may be a virtual area) and the Private Security Business Act.

Formal interviews of staff

The conduct of formal interviews is permissible, subject to the overriding requirements relating to respect for an individual's rights as set out in the Constitution of the Republic of Bulgaria, and the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

See above. In addition, an employer should take into account the requirements of the data protection legislation.

Search and seizure of evidence, whether electronic or physical (overt or covert)

Subject to the Constitution of the Republic of Bulgaria, the European Convention for the Protection of Human Rights and Fundamental Freedoms. The concept of 'personal space' should be taken into account. In addition, the safeguarded employer should have due regard to relevant health and safety legislation and the Private Security Business Act when carrying out search and seizure. Overt searches for physical evidence are generally preferable to covert searches as this reduces the likelihood that a claim will be brought by the individual concerned for unfair practices. However, it might be practical to obtain electronic evidence only when the subject(s) concerned are not present, due to the risk that evidence might be tampered with or deleted.

Is it either usual or necessary to involve the police in investigations?

It is not necessary to involve the police in each case of surveillance and safeguarding, although for criminal matters it is mandatory to involve them, even if the surveillance is being handled internally.

		<p>If the police are involved, at what stage in the investigation does this generally occur?</p> <p>The decision as to when and if to involve the police may depend on a number of factors such as the severity of the matter; the speed of response required (the police may not have adequate resources); access of the organisation itself to investigation capability (typically, small organisations may be less able to respond to an incident than a large organisation with pre-defined resources and processes). In any case, when there are data on a committed violation of public order or a crime the police should be notified immediately.</p> <p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>In Bulgaria, as in the UK, the police have limited resources and therefore cannot realistically investigate all cases in detail. An organisation may undertake its own investigation, alone or in conjunction with a third party, provided that all activities comply with the applicable Bulgarian legislation.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>Suspected violations of public order or criminal activities should be reported to the police immediately. The Measures Against Money Laundering Act imposes duties on persons working in the regulated sector to disclose any knowledge or suspicion of money laundering. Large financial penalties may be applied to those who fail to report suspicions.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

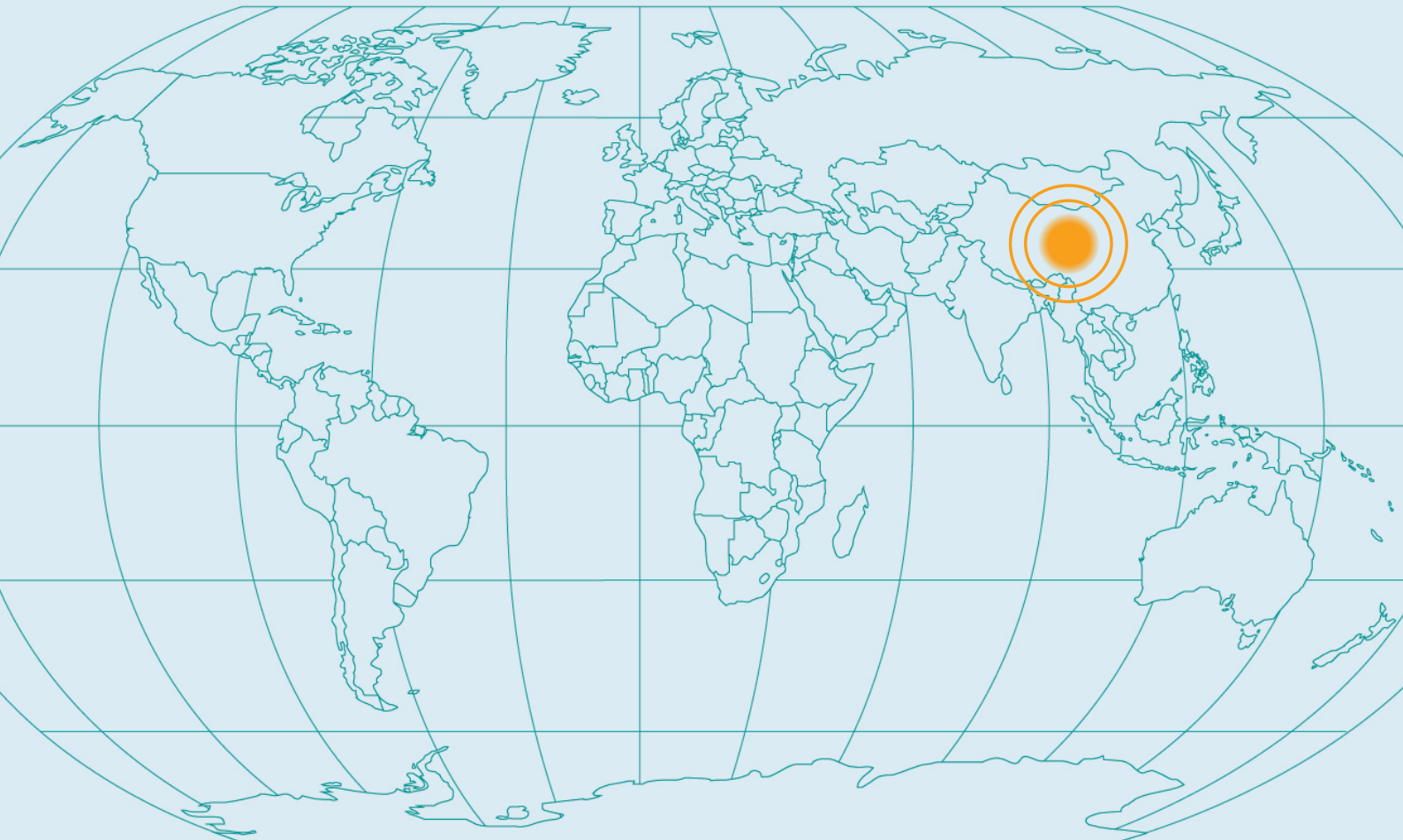
CPNI

Centre for the Protection
of National Infrastructure

SECURITY WATCHDOG
Part of Capita plc

China (People's Republic of)

Personnel Security in Offshore Centres



● China (People's Republic of)

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1

Introduction

This section relates to the mainland People's Republic of China and does not include Special Administrative Regions such as Hong Kong and Macau. Such regions will have different processes, procedures and methods of record keeping and should therefore be treated as separate. As an established commercial and financial hub, Hong Kong has more sophisticated practices than mainland China and HR attitudes are more corporate in nature.

Historically, pre-employment screening in China has been restricted to a limited number of government institutions. However, in recent years the country has opened up as one of the world's leading global markets and has therefore seen a significant influx of Western organisations investing in operations on the Chinese mainland. In China there has been a recent growth in the application of pre-employment security screening as Western organisations seek to implement best-practice HR procedures across all of their international operations.

Like many countries there are practical limitations to pre-employment screening options in China including provincial variations in procedures, lack of complete, centralised databases, restricted access to certain types of data (for example, criminal records or credit records), and the need to rely on local officials (such as the Public Security Bureau) to validate identity documentation.

A number of laws and regulations exist that lay down the rights of employees and employers in relation to both pre-employment security screening and ongoing personnel security measures; primarily the Labour Contract Law of the People's Republic of China. The legal framework in China is not always precise and is open to interpretation. It is generally possible to implement physical security measures such as access controls, although the legality of some forms of monitoring of employee activity is not well defined. Employers should seek local legal advice in relation to specific matters where there is any doubt.

In China, employee investigations are normally carried out by the police or procurator. However, resources remain limited, meaning that ordinarily police will focus their resources on public organisations or matters involving corporations in which there is a high degree of public interest. The private investigation industry in China remains unregulated, so caution should be exercised when organisations elect to conduct investigations themselves, since laws concerning the rights of individuals and employers are imprecise.

In mainland China, records are held by different authorities at a number of levels (local, county, municipal, district, provincial, national, etc). In rural areas, records are not maintained in a way that facilitates their retrieval. Typically, different filing requirements exist in each rural administrative region. However, there is a trend towards improvement of record keeping by ministries, including the conversion of manual records to electronic format. This might not necessarily involve construction of databases, but rather a digitisation of paper-based records.

		<p>Local security concerns</p> <p>In China corporate fraud tends to receive less attention from public investigative bodies owing to limited resources. Therefore it is recommended that employers apply vigilance to protect company assets.</p>
2	Personnel security measures during recruitment	
2.1	Culture of screening	<p>Historically, pre-employment screening was undertaken only by certain government and quasi-government agencies for specific sensitive roles; however, an upsurge in Western companies operating within China, bringing with them common Western employment practices, has seen an increase in the use of screening at the pre-employment stage.</p> <p>Some companies choose only to employ pre-employment screening for positions above a certain level or those requiring a higher level of security (e.g. management, directors, technical positions) and the level of screening will usually increase with the level of responsibility or sensitivity the role requires.</p>
2.2	Major laws and regulations applying to pre-employment screening	<p>Labour Contract Law of the People’s Republic of China, ratified by the Standing Committee of the National People’s Congress, 2008 (amended 2012) (中华人民共和国劳动合同法,全国人大常委会, 2008)</p> <p>Under Article 8, the employer has a right to acquire basic information pertaining to the employee that is directly related to the labour contract. The employee is obliged to provide such information. The law translates literally as:</p> <p>‘The employer shall truthfully advise the scope of work, the working conditions, the place of work, occupational hazards, production safety conditions, labour compensation and other matters requested by the employee; the employer shall be entitled [to receive] from the worker basic information that directly relates to the employment contract, and the employee shall truthfully provide the same.’</p> <p>In practice, the law is subject to interpretation. It is unlikely that Chinese employees would seek redress in a court (as this is not a popular remedy in this culture). Each party is more likely to apply its own understanding of ‘reasonableness’.</p> <p>Administrative Measures for the Post-holding Qualifications of Senior Management of Financial Institutions, issued by the People’s Bank of China, 2000 (金融机构高级管理人员任职资格管理办法, 中国人民银行, 2000)</p> <p>Article 16 requires a comprehensive check of the applicant, covering his/her morality, professional capacity, management capacity and work performance, degrees, professional certificates and identity card.</p>

		<p>Interpretation of the Supreme People’s Court on Several Issues about the Trial of Cases Concerning the Right of Reputation, Supreme People’s Court, 1993 (最高人民法院关于审理名誉权案件若干问题的解答, 最高人民法院, 1993)</p> <p>Article 7 defines ‘infringements on the rights of reputation’. When private information is published in an oral or written way without the consent of the relevant person, and the reputation of the individual is damaged, the provider may be subject to prosecution.</p>
3	Pre-employment checks	
3.1	Identity check	<p>In most cases, a National Identity Card, and in some areas – see below – a local social security card, are preferred forms of identification in China (given their security features). The passport is a much less common form of identification in China.</p> <p>Marriage, birth or adoption certificates are not official forms of identification since they are not issued by the Ministry of Public Security.</p> <p>Legally valid identification is conferred by identity documents issued by the Ministry of Public Security, which include:</p> <ul style="list-style-type: none"> • the household register book (Hukou) • the ID card and • a passport.
		<p>In major cities like Beijing and Shanghai, a social security card issued by the local social security administration may also be an important identification document.</p> <p>There are generally no legal restrictions that prohibit employers from undertaking identity checks, but the identity check must be proportionate and not invade the prospective employee’s personal privacy, such as their home life.</p> <p>Because there are many different types of identification and various issuing authorities inconsistencies may arise. There are also a large number of counterfeit documents in circulation.</p> <p>If an official form of identification cannot be provided by a prospective employee, the employer may confirm the individual’s identity through the Ministry of Public Security (with the individual’s written consent).</p> <p>Identification information can be verified through Public Security Bureaux (PSBs).</p>

3.2

Checks on eligibility to work

Foreign workers

All foreign passport holders are subject to work permit regulations should they wish to seek employment in mainland China. Failure to abide by these rules may result in the individual being detained, repatriated and barred from China for five years.

This is governed by the **Regulations on the Management of Employment of Foreigners In China, Ministry of Foreign Affairs 1996** as follows:

Article 5: organisations that employ foreigners must apply for permission to employ these foreigners and may do so only after obtaining Certificates of the People's Republic of China Permitting the Employment of Foreigners (hereinafter referred to as certificates of permission).

Article 9: foreigners meeting one of the following conditions can be exempted from having to be covered by certificates of permission and employment certificates:

- 1 foreign experts and management personnel engaged with funds directly from the Central Government or with funds from state organs or institutional units, foreign experts and management personnel with senior professional titles or certificates of special skills acknowledged by authoritative technical management departments or trade associations in their home countries or international organizations, and foreigners carrying certificates of foreign experts issued by the Administration of Foreign Experts;
- 2 foreign labourers with Permits for Foreigners to Engage in Offshore Oil Operations in the People's Republic of China who are engaged in offshore oil operations and do not need to come ashore, and who have special skills; and
- 3 foreigners putting on professional art performances under Permits for Temporary Performances of a Business Character as approved by the Ministry of Culture.

Article 10: foreigners meeting any of the following conditions can be exempted from having to be covered by certificates of permission and can, on the strength of occupation visas, apply directly upon entry into China for employment permits and other relevant certificates:

- 1 foreigners who are employed to work in China under agreements and protocols signed between China and foreign governments or international organizations, or who are employed to implement Sino-foreign cooperative projects or projects of exchange; and
- 2 chief representatives and representatives of the residential offices of foreign enterprises in China.

A work permit for foreign employees is usually obtained by the employer before the employee joins the company.

Enquiries regarding work permits can be made to labour and social security bureaux in the relevant jurisdiction.

		<p>For prospective foreign employees, validation of a work permit can be undertaken at the local labour and social security bureau where the work permit was issued. The employer should present the introduction letter (reference letter or delegation letter) under seal together with the identity card of the representative.</p> <p>Local residents</p> <p>Local residents in Shanghai are issued with a Labour Handbook that records their employment, training and benefits history. The Labour Handbook is a prerequisite document throughout the pre-employment process.</p> <p>For prospective domestic employees, Labour Handbooks are usually issued by the urban sub-district administrative office, neighbourhood, township or village labour service centre governing the area in which the prospective employee lives. These organisations can also validate Labour Handbooks.</p> <p>Small private businesses may not file employee documentation with the labour bureau; accordingly, the Labour Handbook might not record every previous employment of a prospective employee.</p>
3.3	Residency checks	<p>Employers do not usually perform residency checks in China. Every Chinese national identification card bears an officially registered address (though this may differ from the individual's current home address).</p> <p>Verification normally includes taking a photocopy of the individual's national identification card, household register page, passport or local social security card.</p> <p>PSBs might help with residency checks, although their cooperation is not guaranteed.</p> <p>To access residency data, employers must obtain consent from the candidate and then approach the local PSB officially.</p>
3.4	Criminal record checks	<p>Name of certificate</p> <p>Certificate of No-Criminal Record (无犯罪记录证明)</p> <p>Department that holds records</p> <p>There are separate local authorities covering each region.</p> <p>Where to apply within country</p> <p>Each regional PSB (GongAn Ju).</p> <p>There is no list of all the PSBs; however contact details for the Beijing Public Security Bureau are:</p> <p>2 Andingmen Avenue (East), Dongcheng District, Beijing, China.</p>

		<p>How to apply within country</p> <p>The process is different in each city and the individual will need to confirm it with his/her local PSB. Applications can be made in person only.</p> <p>Required documents vary at each PSB; however the following are usually required for non-Chinese nationals:</p> <ul style="list-style-type: none"> • original passport with residence permit • photocopies of the passport photo page, Chinese visa and Chinese entry/exit stamps • original work permit • original temporary residence registration form and • original letter of verification issued by the employer stating that the individual has no criminal record.
		<p>Who can apply</p> <p>Individuals and employers or third parties can apply to PSBs in Beijing or Shanghai (this may not be possible at other PSBs).</p> <p>Cost, payment and turnaround</p> <p>The cost varies at each PSB.</p> <p>The fee must be paid in cash in local currency.</p> <p>The turnaround time varies at each PSB. For Beijing and Shanghai, the turnaround time is 7–15 working days.</p> <p>Legislation</p> <p>No specific provisions in the current laws, rules or regulations apply to criminal record checks.</p> <p>Further information can be obtained from the CPNI guidance on <i>Overseas Criminal Record Checks</i> which can be found at http://www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>

3.5	Education checks	<p>Education checks may be undertaken directly with the relevant educational establishment. Applications must typically be made in writing and provide all known information, e.g. full name, date of birth, subject of study. Many organisations have standard processes for dealing with reference enquiries. It is common practice in China for an educational establishment only to release information on educational background to a prospective employer on written consent of the prospective employee.</p> <p>In China, there is no legal obligation on the employee to provide educational or employer references. If employees misrepresent themselves it is possible to dismiss them. Culturally, referees are not obliged to provide references on prospective employees.</p> <p>A request can either be made by letter or by phone, depending on the handling personnel. Confirmation can be given orally or in a letter.</p> <p>Where the educational establishment is not well known, it may be necessary to undertake additional checks to verify the authenticity of the information. Employers should be particularly aware of the risk of fake establishments and/or fake qualifications issued by such establishments.</p>
3.6	Qualification checks	<p>See also Section 3.5.</p> <p>Most professional bodies issue directories of members, so any qualifications claimed can be verified directly with the professional body. It is also important to verify that an individual is an active member of a professional body and has not left nor been removed from membership. Information may be available online and consent of the individual is not generally required in these circumstances. Certain organisations claiming to be professional associations may not be an established organisation. Caution should be applied.</p> <p>Fake documentation is widespread and it is regularly reported that a proportion of employment candidates lie about or over-exaggerate qualifications. For example, attendance at an educational establishment does not mean that the individual graduated from that establishment.</p> <p>Further information can be found from the Administrative Measures for Archives of Institutions of Higher Education (高等学校档案管理办法) at www.moe.edu.cn.</p>
3.7	Employment references	<p>Employers usually ask for contact numbers and/or emails of the prospective employee's references from his/her previous employment. Character references may be requested, but they might not be provided by the referee.</p> <p>In most cases, employers will not provide information on ex-employees' salaries, performance review records or sickness records. Nonetheless, employers may require a certificate of health or sponsor a pre-employment health check for the prospective employee as part of the conditions for a formal employment relationship.</p> <p>Information regarding 'state secrets' or 'classified information' or 'privacy' cannot be obtained.</p>

		<p>Requests for information are made directly to the employer/line manager/referee. The individual’s consent is generally required.</p> <p>If the previous employer is not well known, it may be necessary to undertake additional checks to verify its existence/background.</p> <p>A certificate of health from a recognised 3A-grade hospital in China (or a hospital designated by the employer) may be obtained if required. The pre-employment health check will usually be coordinated by the HR department with the relevant hospital during the prospective employee’s probation period.</p> <p>Character references from previous employers</p> <p>Character references may be taken up depending on the position/ profession applied for.</p> <p>Many referees will be reluctant to provide information regarding the subject’s character since employers are generally cautious about commenting on others. In Chinese culture people will generally give positive references. Furthermore, employers are increasingly prohibiting the provision of character references and comments on performance, whether written or verbal.</p> <p>Character references are not always provided by previous employers who may offer only verification of basic employment history and reason(s) for leaving.</p> <p>Character references from persons of standing in the community</p> <p>Character references can be requested from persons of standing in the community, although this practice is less common in China. Where necessary, such references may be obtained from a local community committee or local police station if they have good knowledge of the subject.</p> <p>It may be necessary to verify the position of the person providing the reference.</p> <p>This might be time-consuming and not cost-effective.</p>
<p>3.8</p>	<p>Financial/ credit checks</p>	<p>These checks may be used for more senior roles and in particular those that involve access to financial systems or controls. Financial/credit checks might be made in the pre-employment screening stage; on an ongoing basis more regularly; or where suspicions/concerns arise.</p> <p>Written consent from the individual for disclosure of their credit information is generally required.</p> <p>The People’s Bank of China (PBOC) maintains a database of corporate and individual credit profiles. However, the database is not publicly accessible. Written consent must be obtained from the prospective employee, who has to be physically present in order to request his/her own credit profile.</p>

		<p>For further details see Instructions of the People’s Bank of China and the Ministry of Information Industry on the Pooling of Enterprise and Individual Credit Information as Shared by the Commercial Banks and Telecommunications Enterprises, People’s Bank of China, 2006 (中国人民银行、信息产业部关于 商业银行与电信企业共享企业和个人信用信息有关问题的指导意 见, 信息产业部 (含邮电部) (已撤销), 中国人民银行, 2006).</p> <p>Interim Measures for the Administration of the Basic Data of Individual Credit Information, issued by People’s Bank of China, 2005 (个人信用信息基础数据库管理暂 行办法, 中国人民银行, 2005).</p> <p>Prospective employers should apply caution in using third-party vendors to obtain ‘credit reports’ because these are unofficial reports and information contained might have been acquired through inappropriate channels.</p>
3.9	Substance abuse screening	<p>Screening for substance abuse is not a common practice in China. Where it is used, it may be part of ongoing security: either as random screening or where there is suspicion of substance abuse.</p> <p>Explicit consent of the individual would be required.</p> <p>Caution should be exercised as the subject may claim reputational damages if errors are made.</p>
3.10	Occupational health checks	<p>The individual should provide their health check record during the job application process; especially where health issues could cause physical risks to other individuals (e.g. air crew, restaurant staff, food preparation and hospitality in general). Usually, the prospective employer will arrange for a health check to be undertaken in a designated hospital before the individual concerned is employed.</p>
4	Personnel security measures during employment	
4.1	Legal requirements	<p>In China there are a number of laws that may limit the options open to an organisation seeking to implement employee security procedures. The list below indicates a number of the most important laws; it is not exhaustive and, given the complexity of law and regulation in China, legal advice should be sought in specific circumstances.</p> <p>The Chinese Constitution contains the following Articles that are relevant to personnel security measures during employment:</p> <ul style="list-style-type: none"> • Article 38: safeguarding a citizen’s basic human rights and dignity • Article 39: protecting citizens from unlawful search or trespass and • Article 40: protecting a citizen’s freedom and secrecy of personal communication: see www.gov.cn/ziliao/flfg/2005-06/14/content_6310_3.htm. <p>The Chinese Civil Procedure Law (www.china.org.cn/english/government/207343.htm) contains Article 101 protecting citizens from defamation.</p>

		<p>The Chinese Criminal Law contains the following relevant Articles:</p> <ul style="list-style-type: none"> • Article 245: provisions on body search and trespassing • Article 246: provisions on defamation, libel and slander and • Article 252: provisions on hiding, destroying or illicitly opening other people’s mail. <p>The Juvenile Protection Law includes Article 39 protecting a juvenile’s privacy: see www.gov.cn/ziliao/flfg/2006-12/29/content_554397.htm.</p> <p>The Lawyer’s Law includes Article 35 protecting lawyers’ rights in the course of collecting evidence: see www.gov.cn/flfg/2007-10/28/content_788495.htm.</p> <p>The Labour Law 1995 includes the following relevant chapters:</p> <ul style="list-style-type: none"> • Chapter VI: working conditions and workplace safety • Chapter X: dispute resolution • Chapter XI: inspection and scrutiny and • Chapter XII: legal liabilities. <p>See http://news.xinhuanet.com/employment/2007-12/17/content_7266586.htm.</p> <p>The Implementation Measures of the Labour Contract Law 2008 includes the following relevant Articles:</p> <ul style="list-style-type: none"> • Article 8: about containing identity and address information in the labour contract and • Article 26: dismissal for fraudulent acts. <p>See www.gov.cn/zwgk/2008-09/19/content_1099470.htm.</p>
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	<p>The Labour Contract Law of the People’s Republic of China protects employers’ rights regarding trade secrets and intellectual property accessed by employees during an employment relationship. Employers can include appropriate clauses in employees’ labour contracts/ agreements.</p> <p>Further information is available at www.gov.cn/ziliao/flfg/2005-08/05/content_20968.htm.</p>
4.4	Local legislation that specifically governs the rights of the employee	<p>Both the Criminal Law and the Labour Law of the People’s Republic of China contain clauses protecting the rights of employees, including rights to compensation, work time, social insurance, working conditions and safety.</p> <p>The Constitution of China also protects individuals’ privacy and personal communication, which may restrain investigations imposed by the employer on its employees.</p> <p>See www.gov.cn/ziliao/flfg/2005-06/14/content_6310_4.htm</p>

4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	Individuals may bring claims against their employer through the local work safety watchdogs or labour unions. However, it should be understood that Chinese labour unions do not report to workers, they report to the government and specifically the Communist cadres.
4.6	What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?	<p>In China it is illegal to dismiss a member of staff because the employee is:</p> <ul style="list-style-type: none"> • pregnant, nursing or on maternity leave • receiving prescribed treatment for illness or injury • suffering from occupational diseases or work-related injuries or • violating rules (with no evidence to back up the employer's claim). <p>Employees may bring a claim for unfair dismissal against their employer to the labour tribunal.</p>
4.7	Availability of security measures	<p>The sanction for breaches of particular laws or regulations relating to ongoing personnel security matters varies; most commonly this includes fines or warnings, followed by closure of the business. Prison is an available, although less commonly used, sanction. The application of specific laws in this area is not always clear, and employers are advised to seek legal advice in relation to specific circumstances.</p> <p>Restriction of access to the premises</p> <p>In the Chinese constitution trespassing is prohibited under provisions regarding property rights. For non-residential premises, the implementation of access controls is a commonly accepted practice in China.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>This measure is generally available although Chinese laws are not necessarily always clear in this regard.</p> <p>Physical screening (on entry/exit)</p> <p>Physical screening is more commonly practiced at factory premises and less so at office buildings.</p> <p>Prohibition of removal of data from the premises (hard-copy)</p> <p>Guidance regarding archiving and preserving records is issued by ministries or national supervisory bodies and applies to their subordinate institutions respectively. There is no central data protection law, however, although the seventh amendment to the Criminal Law has introduced penalties for misuse of personal data. This is a developing area.</p>

		<p>Prohibition of removal of data from the premises (electronic)</p> <p>See 'hard-copy' above.</p> <p>Visual surveillance (CCTV or other cameras), either overt or covert</p> <p>Legislation in this area is unclear. Companies may install CCTV at their own discretion, although caution should be exercised, and legal consultation should be sought in specific circumstances.</p> <p>Overt monitoring of access to IT and other equipment</p> <p>Legislation in this area is somewhat unclear, but companies do generally apply overt monitoring of access to IT and other equipment without infringing personal security and privacy.</p> <p>Covert monitoring of access to IT and other equipment</p> <p>Covert monitoring of access to IT and other equipment is used in China, although the legislation is unclear.</p> <p>Reporting hotlines (anonymous)</p> <p>The PSBs or procurators operate hotlines and handle anonymous whistleblowing calls. Identification will generally be requested, although the whistleblower may insist on remaining anonymous. Legislation in this area is unclear.</p> <p>Reporting hotlines (confidential)</p> <p>Private companies may set up their own confidential whistleblowing hotlines, but must not transmit information that concerns 'state secrets' or infringes individuals' privacy.</p> <p>Use of alerts/automated warning systems to identify unusual employee behaviour (out-of-hours activities, duplicate payments)</p> <p>Legislation in this area is unclear and specific legal guidance should be sought.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>Legislation is unclear in this area. In practice, companies may monitor communications transmitted via their own IT facility, but must not invade individuals' privacy. Caution and legal consultation is recommended as some individuals have been successful in claiming damages.</p>
4.8	Formal investigations	<p>The application of specific laws in this area is not always clear, and employers are advised to seek legal advice in relation to specific circumstances.</p> <p>It is good practice to apply the UK rationale that actions by an employer should be proportional and necessary. However, as the law is not clearly defined, in practice it is possible to undertake any procedure provided (a) the employer is not being sued and (b) the matter does not involve 'state secrets'.</p>

Is there a licensing regime covering investigators?

The Central Commission for Discipline Inspection of the Chinese Communist Party is recognised as the major body of investigators. At present, there is no formal legislation on the private investigations industry. In general, private investigators operate in a grey area.

Physical surveillance (overt or covert)

Legislation in this area is unclear. Physical surveillance should only be carried out by official government investigators. However, the definition of 'surveillance' is not clear and therefore subject to legal interpretation.

Electronic surveillance (e.g. tracking devices)

Legislation in this area is unclear. In China the conduct of electronic physical surveillance by a private organisation may be illegal and caution should be exercised. Appropriate legal advice should be sought in this area.

Visual and communication surveillance (using cameras, video or CCTV)

CCTV is widely used in factory premises and office buildings in China. Use of covert surveillance will be subject to legal provisions regarding individuals' privacy. Privacy laws in China are weak, however, and employers generally do not inform employees that they are being monitored.

Communication intercept (including oral, written and electronic communication including bugging devices)

Legislation is unclear as the private investigations industry is not adequately defined. Provisions under the Criminal Law strictly prohibit 'illicit use' of 'bugging devices'.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

The area of computer or database surveillance is not clear and legislation is pending. Electronic evidence is admissible in court, though definitions and acquisition of such evidence are subject to legal interpretation.

Formal interviews of staff

Formal interviews are common practice in China, but there are no clearly defined, standard procedures for documenting the interview. Caution should be exercised to avoid invasion of privacy.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

Any such surveillance can only be carried out by official investigators, i.e. the police or procurator.

Search and seizure of evidence, whether electronic or physical (overt or covert)

Legislation in this area is unclear. Currently, other than public investigators, only lawyers are entitled to carry out search and seizure of evidence under the Lawyer's Law. The concept of 'personal space' should be taken into account when conducting investigations. Overt searches for physical evidence are generally preferable to covert searches as this reduces the likelihood that a claim for unfair practices will be brought by the individual concerned.

Can those procedures above that are not legally permissible be conducted under direction of a court order?

Court orders are usually only given to public investigative bodies, i.e. the police or procurators.

Is it either usual or necessary to involve the police in investigations?

It is not necessary to involve the police in all investigations although for criminal matters it may be preferable to involve them, even if the investigation is being handled internally. In addition, if an organisation is contemplating bringing a matter before a court, it is preferable to involve the police.

Police are not generally involved in commercial matters unless the employee(s) in question has/have committed a criminal offence that (a) has an impact on general social stability, (b) is against the public interest, (c) involves the protection of 'state secrets' or (d) concerns other matters seen as sensitive in the government's judgement.

There is no specific restriction on the involvement of corporate investigators, or private investigators hired by a company to conduct investigations work. The results of their work may be handed to the police.

If the police are involved, at what stage in the investigation does this generally occur?

The police might or might not be involved in an investigation. The decision as to when and if to involve the police may depend on a number of factors such as the severity of the matter; the speed of response required (the police may not have adequate resources); access of the organisation itself to investigation capability (typically small organisations may be less able to respond to an incident than a large organisation with pre-defined resources and processes).

		<p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>In China, the police have limited resources and therefore cannot realistically investigate all cases in detail. An organisation may undertake its own investigation, alone or in conjunction with a third party. Where an investigation is likely to progress to a criminal complaint, it is essential that the investigation is conducted to criminal standards. This includes the gathering of physical and electronic evidence, preferably with police involvement. Information that is not gathered to an adequate criminal standard may be inadmissible in court. The police may be dissuaded from taking on a case unless they can be certain that information has been gathered to criminal standards, or they have been involved from the outset.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>Legislation in this area is unclear. In general, employers – as corporate citizens – are asked to report any matters that concern ‘state secrets’, espionage or any activities that may impact on social stability (foreigners are not expected to have access to ‘state secrets’). Also, criminal penalties may be applied to those who fail to report suspicions of money laundering. Organisations should watch out for the latest rules or regulations as they are issued by different ministries or government regulatory bodies.</p> <p>Other legal considerations not covered above.</p> <p>Legislation concerning the governance of the private investigations industry in China is developing. The conduct of investigations should take account of changes in this area of Chinese law and regulation.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories CPNI Guidance Documents</p>

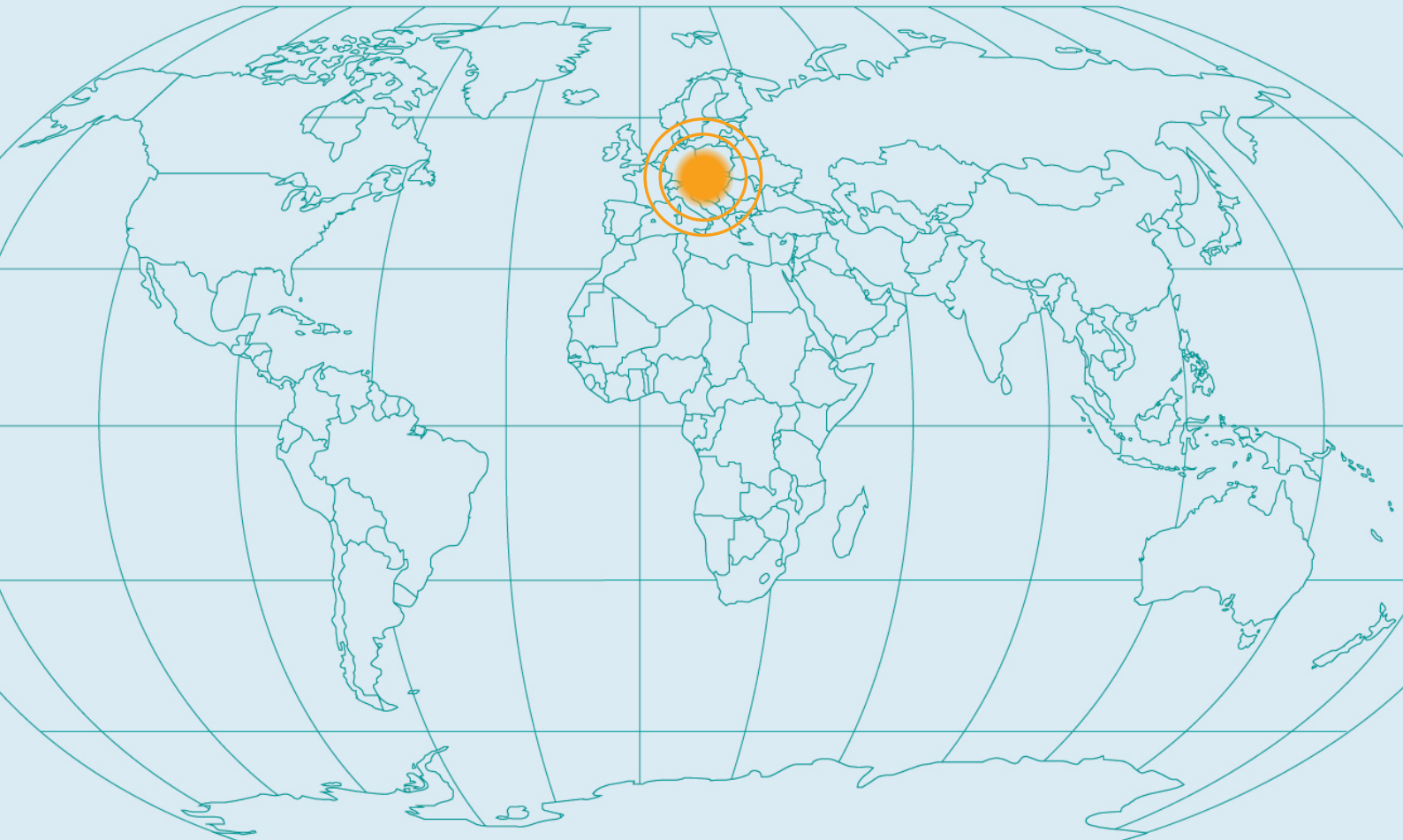
CPNI

Centre for the Protection
of National Infrastructure

SECURITY **WATCHDOG**
Part of Capita plc

Czech Republic

Personnel Security in Offshore Centres



Czech Republic

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

<p>1</p>	<p>Introduction</p>	<p>The Czech Republic is a popular location in Europe for outsourcing. It is attractive to companies seeking to offshore or outsource their operations for a number of reasons, including its:</p> <ul style="list-style-type: none"> • geographical proximity to Western European markets • cultural links to Western Europe • strong IT and communications infrastructure and relatively mature IT services industry • lower geopolitical risks and • foreign language skills, in particular German. <p>Employers may undertake a range of measures to verify the background of a job candidate as part of the pre-employment security screening process. Such measures are subject to data protection legislation designed to protect individual rights. Both employers and employees in the Czech Republic are subject to the conditions of the Labour Code, which imposes rights and duties on both parties.</p> <p>In relation to ongoing personnel security measures, an employer’s ability to undertake certain security measures (such as surveillance activities – whether physical, visual, electronic or communications) is restricted under the Labour Code and the availability of such measures will be determined by whether they are proportionate to the perceived risk. For example, an employer may be able to utilise such measures where the purpose is to detect or investigate suspected criminal activities. It is good practice for an employer to inform employees of proposed security measures.</p>
<p>2</p>	<p>Personnel security measures during recruitment</p>	
<p>2.1</p>	<p>Culture of screening</p>	<p>In the Czech Republic the ability of an employer to undertake pre-employment security screening measures is restricted by a number of laws and regulations:</p> <ul style="list-style-type: none"> • the Civil Code (which protects individual privacy) • the Personal Data Protection Act (which requires an individual to give consent to the processing of their personal data) and • the Labour Code (which imposes limits on what an employer may request before conclusion of an employment contract). <p>For example, the Labour Code prevents employers from seeking information about family or personal property details; membership of political movements; or (unless prescribed by law) the criminal history of employees. An individual may submit a request for his/her own criminal record, the authenticity of which may be verified online by a prospective employer.</p> <p>Increased levels of background screening are applied to individuals with access to confidential and/or sensitive data, provided the individual has given consent.</p>

2.2	Major laws and regulations applying to pre-employment screening	<p>In the Czech Republic the principal legislation governing and/or restricting the application of prospective employee screening is as follows:</p> <ul style="list-style-type: none"> • The Civil Code, Act no. 40/1964 Sb., (as amended). Section 4 of the Code defines the right of an individual to the protection of their privacy. This impacts on pre-employment screening: prospective employers cannot invade the ‘private space’ of the candidate by collecting information of a private nature about the candidate unless he or she knowingly consents to this. • The Personal Data Protection Act, no. 101/2000 Sb. governs the rights and duties of a data controller in relation to processing personal data and the conditions for sharing data across borders. The Office for Personal Data Protection is an independent body that is involved in the supervision of data protection issues, and that investigates complaints of alleged infringements of the data protection legislation. In pre-employment security screening, prospective employers may only gather and process the personal data of job applicants with the candidate’s consent, and the procedure undertaken must accord with applicable legislation. For more details, see the Office’s website at: www.uoou.cz/en/.
3	Pre-employment checks	
3.1	Identity check	<p>It is usual to undertake identity checks (given name, date of birth, parents’ names and addresses) against ID documents presented by the applicant.</p> <p>The Personal Data Protection Act establishes strict rules regarding the processing of personal data. It is only possible to process personal data with the consent of the person concerned or where provided for by law.</p> <p>In the Czech Republic commonly accepted forms of identification include:</p> <ul style="list-style-type: none"> • national ID cards • passports and • birth certificates.
3.2	Checks on eligibility to work	<p>Work permit and nationality checks</p> <p>Ss 89–101 of the Employment Act stipulate that foreigners can only be hired and employed provided they have a valid permit to stay, a work permit or hold a green card.</p> <p>Work permits are issued by the relevant employment office based on information provided by both the employer and the prospective employee.</p> <p>Employers can ask prospective employees to provide work permit documentation, provided the candidate already holds a work permit. Alternatively, the employer may assist the prospective employee to obtain the appropriate work permit.</p> <p>Further guidance regarding work permits for foreigners is available at www.mn.domavcr.cz/advice-for-living-in-the-czech-republic/employment.</p>

3.3	Residency checks	<p>An individual's residential address is shown on their ID card. There is a legal requirement to keep this address up to date. In practice this does happen, and generally employees are required to advise employers of any change of address.</p> <p>The Personal Data Protection Act sets out strict rules regarding personal data processing. It is only possible to process personal data with the consent of the person concerned or in cases provided for by the law.</p> <p>Apart from the national ID card, no other sources of information in the Czech Republic (such as the electoral roll) are publicly available.</p>
3.4	Criminal record checks	<p>Name of certificate</p> <p>Extract of Criminal Record (Opis z Rejstříku Trestů)</p> <p>Department that holds records</p> <p>Criminal Register of the Czech Republic (Rejstřík trestů)</p> <p>Where to apply within country</p> <p>Rejstřík trestů, Soudní 1, 140 66 Praha 4, Data Box: vtqabcz, Czech Republic.</p> <p>Email: rejstrik@rejtr.justice.cz Website: http://portal.justice.cz</p> <p>How to apply within country</p> <p>In person</p> <p>At a contact point of the CzechPOINT system (local and municipal authority, branch office of the CzechPost or the Czech chamber of commerce, notary). Addresses and business hours of contact points are given on www.czechpoint.cz/. Extracts from the Criminal Register issued by contact points of the CzechPOINT system are primarily designed for use within the Czech Republic. For use outside the Republic an extract should be obtained directly from the Criminal Register (see above).</p> <p>From a local and municipal authority. Addresses and business hours of local and municipal authorities are available at http://portal.gov.cz.</p> <p>From the Criminal Register of the Czech Republic (see above).</p> <p>Online</p> <p>At http://eservice-fo.rejtr.justice.cz/webform/ (only for holders of valid electronic signature).</p> <p>Verifying identity – in person</p> <p>An individual's identity is verified by an original and valid form of ID (e.g. citizen's identity card, passport, foreigner's residence permit, etc) that carries a photograph of the individual.</p>

Third parties applying on behalf of an individual must provide an officially authenticated power of attorney in Czech.

The information presented in an application is verified by reference to the original of a valid ID containing at least the name, current surname and surname at birth, date and place of birth, birth number and state citizenship of the individual. If any data is missing the individual or a third-party representative can submit a birth certificate, birth and baptism certificate, confirmation of birth, marriage certificate, etc.

Citizens of the Czech Republic and the Slovak Republic must submit original documents or their officially authenticated copies. Citizens of other states must submit original documents or officially authenticated copies, including sworn translations into the Czech language.

Verifying identity – online

As for applications in person; however, scanned copies of original documents are acceptable.

Who can apply

- Individuals.
- Employers can apply on behalf of an individual provided that the individual grants an officially authenticated power of attorney to the employer.
- Third parties can apply on behalf of an individual provided that the individual grants an officially authenticated power of attorney to that party.

Cost, payment and turnaround

Cost

CZK 100.

Payment methods

Payment can be made:

- in cash or
- a holder of a valid electronic signature may make a transfer payment; a bank account within the Czech Republic is not required.

Turnaround

Certificates can usually be issued immediately except in the following circumstances:

- if the Criminal Register extract requested needs to contain records from other EU member states or
- for persons born in the territory of the Slovak Republic who do not hold Slovak citizenship and whose records have not been yet transferred from the Criminal Register of Bratislava to the Criminal Register of Prague, in which circumstances:
 - an extract processed on the basis of the request filed with the Criminal Register of the Czech Republic is posted to the individual's address and
 - this may delay supply of the extract by up to a week.

		<p>Legislation</p> <ul style="list-style-type: none"> • Act No. 269/1994 of the Collection of Laws (Coll.) on the Criminal Register • Act No. 40/2009 (Coll.) Penal Code • Act No. 141/1961 (Coll.) on Criminal Procedure • Act No. 101/2000 (Coll.) on Protection of Personal Data • Act No. 499/2004 (Coll.) on archives and records management and on amendments to certain laws • Act No. 500/2004 (Coll.) Administrative Procedure Code and • Personal Data Protection Act. <p>The Office for Personal Data Protection exercises the competence of a supervisory authority in the area of personal data protection: its address is</p> <p>The Office for Personal Data Protection Pplk. Sochora 27,170 00 Praha 7</p> <p>Further information can be obtained from the CPNI guidance on Overseas Criminal Record Checks which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>
3.5	Education checks	<p>Employers may seek information on education background to establish whether a prospective employee has attended the educational establishments claimed.</p> <p>Documentation detailing an individual’s education history is usually provided by the prospective employee. In practice this information is rarely verified with educational institutions.</p> <p>Under the Personal Data Protection Act, an employer must obtain the consent of the individual to make enquiries directly with relevant education establishments.</p> <p>Educational institutions are not obliged by law to provide/confirm such information.</p>
3.6	Qualification checks	<p>Employers may check the qualifications claimed by a prospective employee.</p> <p>See education checks (Section 3.5)</p>
3.7	Employment references	<p>Under s. 313(1) of the Labour Code, on the termination of an employment relationship or an agreement on working activity an employer is obliged to issue the employee with a verification of their employment, which provides:</p> <ul style="list-style-type: none"> • details of employment (specifying whether it was an employment relationship or an agreement on working activity and its duration) • type of work done • employee’s qualifications (the level of professional qualification achieved) • whether the employment was terminated by the employer for severe breach of obligations relating to the work carried out by the employee

		<ul style="list-style-type: none"> • length of employment • any deductions being made from the employee’s wages, stating: <ul style="list-style-type: none"> – in whose favour – the amount of the claim for which further deductions are to be made and – the total deductions already made and the order history of the claims, and <p>Under s. 313(2) the employer is obliged, at the employee’s request, to issue a separate document showing the amount of the employee’s average earnings and other facts affecting assessment of the employee’s entitlement to unemployment benefit.</p> <p>Under s. 314 the employer is obliged, on an employee’s request, to provide him or her with an employment reference within 15 days, but not earlier than two months before the end of the employee’s employment. All documents concerning the appraisal of an employee’s work, their qualifications (skills), capabilities and other facts relating to work performance are regarded as an employment reference.</p> <p>Under s. 314(2) other information not stipulated in s. 314(1) may be provided to a third party (e.g. a prospective employer) with the consent of the individual.</p> <p>Employers are not obliged to issue or confirm references to another legal entity or successive employer, although this often happens informally.</p> <p>Character references from previous employers</p> <p>Prospective employers may take up character references from previous employers.</p> <p>There is no obligation on the previous employer to provide this information. The sections of the Labour Code outlined above (employment references) also apply.</p> <p>Character references from persons of standing in the community</p> <p>These may include persons of standing (e.g. police officers or professionals) who have known the individual for a period of time. It is at the discretion of the individual him- or herself to identify a person to be asked for references, which that person is not obliged to provide.</p>
3.8	Financial/ credit checks	<p>Under s. 316 of the Labour Code an employer may not require from an employee (directly or indirectly through third parties) any information that does not relate directly to work performance and to employment (labour) relationships, including information concerning an individual’s family or property.</p> <p>However, despite the above provision, an employee may give consent for an employer to obtain financial or credit information.</p> <p>An employer can obtain credit information from third-party credit data providers such as SOLUS – the Association for Protection of Leasing and Consumer Credits (with the consent of the individual concerned). Further information on SOLUS can be found at www.solus.cz.</p>

3.9	Substance abuse screening	<p>Screening for substance abuse is not widespread, and is not generally employed by organisations in the Czech Republic.</p> <p>Explicit consent from the individual would be required. However, no specific legal regulation governing this area has been implemented. Any sensitive personal data is subject to the provisions of the Personal Data Protection Act.</p>
3.10	Occupational health checks	<p>Under s. 32 of the Labour Code an employer is obliged, where specifically prescribed by law, to ensure that an individual undergoes a pre-employment medical examination before conclusion of the employment contract. This may be applicable where the individual will be involved in situations where health issues could cause physical risks to other individuals (e.g. train driver, forklift truck operator, etc) as well as for jobs with national security forces (police, army, firemen, etc). The employer, however, is only entitled to information as to whether the prospective employee is able to carry out a the type of job applied for. The employer is not entitled to seek or gather information about prospective employees' health conditions.</p> <p>In general, information concerning an individual's health is classified as sensitive personal information under the Personal Data Protection Act. Sensitive information can be processed only with the explicit consent of the individual.</p>
4 Personnel security measures during employment		
4.1	Legal requirements	<p>The principal legal requirements applying to ongoing personnel security measures in the Czech Republic are set out below:</p> <ul style="list-style-type: none"> • The Charter of Fundamental Rights and Freedoms, Act no. 23/1991 Sb., as amended, defines individuals' basic rights, such as inviolable privacy, private life, employment, family, etc. An individual is thus protected against unauthorised gathering, publication or misuse of personal data. The Office for Personal Data Protection in the Czech Republic has drawn particular attention to the need for proportionate use of camera surveillance systems that might infringe the Charter and in turn the Personal Data Protection Act. It has emphasised that the use of such monitoring systems must be 'necessary' and 'must not infringe on the private and personal life of monitored persons'. • The Office for Personal Data Protection has set out its detailed findings in relation to cases involving the Personal Data Protection Act on its website: www.uoou.cz/en/. • Section 4 of the Civil Code, Act no. 40/1964 Sb., as amended, defines the right of an individual to protection of privacy.

		<ul style="list-style-type: none"> • The Labour Code, Act No. 262/2006 Sb. (as detailed above). There has been some criticism of the Labour Code (for example by the Economic Chamber of the Czech Republic); in particular: <ul style="list-style-type: none"> – increased references to the Civil Code that introduce greater levels of uncertainty – bias towards the rights of the employee and – collective agreements that cover all employees, union members or not. • The Employment Act, Act No. 435/2004 Sb. defines the state employment policy, the rights and duties of the Ministry of Labour and Social Affairs, the powers of employment offices, the right to work, conditions for the activity of job agencies, unemployment contributions and their calculation, conditions for employing disabled persons and foreigners, retraining, investment incentives and other tools for promoting employment policy and conditions for children’s activities. • The Anti-Money Laundering Act, Act No. 253/2008b on Selected Measures against the Legitimation of Proceeds from Criminal Activities and Financing of Terrorism, as amended, implements the Third EU Money Laundering Directive and requires regulated institutions to report suspicions of money laundering to the law enforcement authorities. <p>In practice this legislation limits the application of ongoing security procedures to a great extent. Given the complexities of local laws and regulations, legal advice should be sought in specific circumstances.</p> <p>The largest trade union confederation in the Czech Republic is ČMKOS (www.cmkos.cz/), the successor to the Czechoslovak union confederation, CS KOS. A local trade union is the main form of employee representation in the workplace. In practice, however, trade unions only operate within a minority of companies. Where a union does not exist, a works council may be instituted (these have fewer rights than a trade union).</p>
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	<p>Certain personnel security measures are explicitly mentioned in the Labour Code (see below). In those cases, the rights of the employer are usually defined, although only in a general manner. Security measures not explicitly mentioned by the Code are permitted providing their application cannot be ruled out by the application of other laws (for example, data privacy legislation or protection of privacy under the Civil Code).</p>
4.4	Local legislation that specifically governs the rights of the employee	<p>As for employers, the Labour Code specifically governs the rights of an employee in relation to ongoing personnel security measures.</p>

4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	Individuals may bring claims against their employer under the legislation set out above (Section 4.1). In cases where a local trade union exists, an employee's rights will generally be represented through that union.
4.6	What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?	<p>The Labour Code sets down reasons for which the employee can be dismissed by the employer. The employee can challenge the dismissal in court. An employer must consult the local trade union (if one exists) on redundancies, transfers and health and safety issues. Employers cannot discriminate against employees for belonging to a trade union.</p> <p>Under s. 52 of the Labour Code the employer can dismiss an employee for unsatisfactory work, provided:</p> <ul style="list-style-type: none"> • the employee had been asked by the employer in writing to address the deficiency during the 12-month period prior to dismissal and • he or she failed to address the deficiency in reasonable time. <p>An employee may be given notice of immediate termination by his employer provided that:</p> <ul style="list-style-type: none"> • during the previous six months the employer had warned the employee of this possibility in writing and • the employee had seriously breached a duty arising from statutory provisions and relating to the work done by them.
4.7	Availability of security measures	<p>Restriction of access to premises</p> <p>There are no specific restrictions that apply to restricting access to premises.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>There are no specific restrictions that apply to restricting access to rooms/zones.</p> <p>Physical screening (on entry/exit)</p> <p>Under s. 246 of the Labour Code the employer may list material that may not be brought into or taken away from the premises, provided that the provisions of s.11 of the Civil Code are adhered to. Any physical checks may only be carried out by persons of the same sex.</p> <p>Prohibition of removal of data from the premises (hard-copy)</p> <p>Confidentiality of records may be covered in the employment contract (as governed by the Labour Code – although there are no specific conditions in the Code itself). Relevant provisions of the Personal Data Protection Act, the IP Protection Act and bank secrecy regulations may also apply, depending on circumstances.</p> <p>Prohibition of removal of data from the premises (electronic)</p> <p>See above.</p>

Visual surveillance (CCTV or other cameras), either overt or covert

The use of visual surveillance, both overt and covert, is covered by s. 316 of the Labour Code. An employer is not permitted to use such a measure unless it has a 'serious reason' for doing so.

The Code defines 'serious reason' as something related to the nature of the activities carried out by an employer. However, it does not provide specific guidance as to what nature of activities would justify such measures. Such interpretation would be at the discretion of the courts.

Where a 'serious reason' exists and surveillance is undertaken overtly, an employer has a duty to notify employees of the scope of the surveillance and the method to be used. In cases where covert measures are used (e.g. where an employee is suspected of criminal activity), provided the use of surveillance measures falls within the boundaries of the Labour Code notification to the employee concerned is not required.

Overt monitoring of access to IT and other equipment

See 'Visual surveillance' above.

Covert monitoring of access to IT and other equipment

See 'Visual surveillance' above.

Reporting hotlines (anonymous)

The use of reporting hotlines is not widespread in the Czech Republic although their number and use has increased in recent years. For example, several government ministries have established anti-corruption hotlines both for their own staff and for members of the public.

Reporting hotlines (confidential)

See 'Reporting hotlines (anonymous)' above.

Use of alerts/automated warning systems to identify unusual employee behaviour (out-of-hours activities, duplicate payments)

Although there is no specific prohibition of the use of automated warning systems, they are not widely used in the Czech Republic.

Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)

The monitoring of telephone communications, both overt and covert, is forbidden under s. 316 of the Labour Code unless the employer has a serious reason to implement it, in which case that employer must directly notify its employees of the scope of the monitoring and the method to be used.

4.8

Formal investigations

Is there a licensing regime covering investigators?

There is no official licensing regime in the Czech Republic.

Physical surveillance (overt or covert)

Physical surveillance, whether overt or covert, is forbidden under s. 316 of the Labour Code unless the employer has a serious reason to implement it, in which case that employer must directly notify its employees of the scope of the surveillance and the method(s) to be used.

Electronic surveillance (e.g. tracking devices)

See 'Physical surveillance' above.

Visual and communication surveillance (using cameras, video or CCTV)

Visual and communication surveillance, whether overt or covert, is forbidden under s. 316 of the Labour Code unless the employer has a serious reason to implement it, in which case that employer must directly notify its employees of the scope of the surveillance and the method(s) to be used.

Communication intercept (including oral, written and electronic communication including bugging devices)

Communication interception is forbidden under s. 316 of the Labour Code unless the employer has a serious reason to implement it, in which case that employer must directly notify its employees of the scope of the monitoring and the method to be used. (As noted under 'Visual surveillance' in **Section 4.7** above, 'serious reason' is not defined under the Labour Code. Its interpretation would be at the discretion of the courts.)

Computer or database surveillance (using either hardware or software tools, including forensic tools)

Computer or database surveillance is forbidden under s.316 of the Labour Code unless the employer has a serious reason to implement it, in which case that employer must directly notify its employees of the scope of the monitoring and the method to be used.

Formal interviews of staff

Formal interviews of staff may be undertaken provided the individual consents to this (there is no obligation on employees to consent). Relevant provisions of the Constitutional Act and the Charter of Fundamental Rights and Freedoms will apply to the conduct of interviews. www.usoud.cz/listina-zakladnich-prav-a-svobod/

Even where an employee consents to interview by an employer, the information gathered in such an interview might not be admissible in court proceedings.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

In practice, many employers in the Czech Republic do apply a certain degree of transactional surveillance, of such as telephone, email or access to web sites. This may also include monitoring access to areas within buildings.

Search and seizure of evidence, whether electronic or physical (overt or covert)

Search and seizure of personal belongings is not allowed without advance consent by the individual. Corporate property can be searched and seized as evidence with the consent of the person entitled to act on behalf of the organisation.

Is it either usual or necessary to involve the police in investigations?

It is not necessary to involve the police in investigations although, for criminal matters, it may be preferable to involve them even when the investigation is being handled internally.

If the police are involved, at what stage in the investigation does this generally occur?

The decision as to if and when to involve the police may depend on a number of factors such as:

- the severity of the matter
- the speed of response required (the police might not have adequate resources) and
- investigation resources available to the organisation (small organisations may be less able to respond to an incident than large organisations with pre-defined resources and processes).

Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?

The police have limited resources and cannot investigate all cases in detail. An organisation may undertake its own investigation, alone or in conjunction with a third party. Where an investigation is likely to progress to a criminal complaint it is essential that the investigation is conducted to criminal standards. This includes the gathering of physical and electronic evidence.

Evidence that is not gathered to an adequate standard may be inadmissible in court. The police might be dissuaded from taking on a case unless they can be certain that information has been gathered to criminal standards, or they have been involved from the outset.

What duties does the employer have to report information to local law enforcement authorities?

The Anti-Money Laundering Act imposes duties on persons working in the regulated sector to disclose any knowledge or suspicion of money laundering. Criminal penalties/fines may be applied to those who fail to report suspicions.

	Sources	Open Source Government and Legal Repositories CPNI Guidance Documents
--	----------------	--

CPNI

Centre for the Protection
of National Infrastructure

SECURITY **WATCHDOG**
Part of Capita plc

Hungary

Personnel Security in Offshore Centres



Hungary

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1

Introduction

Although not considered as mature an outsourcing and offshoring destination as some of its fellow European countries, Hungary remains a popular location in Europe for outsourced operations. Outsourcing companies in Hungary are regularly involved in providing IT outsourcing and software services (the largest element of the sector) closely followed by manufacturing, Business Process Outsourcing and HR Process Outsourcing such as back-office administration of payroll systems. This arises from a combination of factors: its labour costs remain some of the lowest within the European Union (EU) and compare favourably with other significant offshore centres such as India and near-shore centres such as Bulgaria; it benefits from a well-educated workforce, with a large pool of graduates. English is widely spoken and the country benefits from close cultural ties with Western Europe. Hungary's membership of the EU also affords greater protection to employers and employees, for example in the area of data protection.

Employment measures in Hungary are governed principally by the Labour Code (see **Section 2.2**). The Labour Code sets down the rules between employees and employers. Recent revisions have been designed to provide greater flexibility in the law away from the collective agreements and for it to be more attractive to foreign investor firms.

Pre-employment security screening measures are generally available to employers in Hungary, and it is common practice (particularly for more senior positions or posts involving access to sensitive materials and in multinationals) to carry out a range of background checks. These measures are subject to personal data protection legislation and anti-discrimination legislation like most European countries. An individual must generally consent to disclosure of personal information, such as employment references or criminal checks. Data protection legislation also applies to the conduct of ongoing employee security measures. Any measures undertaken by an employer should have due regard to data protection legislation which affords protection to personal rights and privacy. All pre-employment security screening measures should be reasonable and proportionate to the job role and carried out with the consent of the individual. As a member of the EU, Hungary has also enacted human rights legislation. Article 8 of the European Convention on Human Rights guarantees an individual's right to respect for private and family life. Any security measures undertaken (particularly those involving possible intrusion into private life, or private 'areas') should take into account such legislation.

2	Personnel security measures during recruitment	
2.1	Culture of screening	<p>Pre-employment security screening measures may be undertaken in Hungary, subject to a number of laws and regulations. In particular, this includes anti-discrimination law, personal data protection law and the Labour Code. Although screening is permissible and is carried out it is not considered as normal practice across all industry sectors and by all companies. Where pre-employment screening is performed, the level of review is generally common across the industry in which the employer is working and the proposed role and responsibilities of the applicant at the employer’s organisation. Both the government sector and several other sectors, such as banking and financial institutions, IT and software services, have established pre-employment security screening procedures. In addition, it is usual for international organisations with operations in Hungary to apply pre-employment security screening as part of their corporate security process that applies to all international operations. Such screening would seek to identify discrepancies in the background of an individual, such as education, qualifications or references.</p> <p>Pre-employment screening is still viewed as alien by the majority of Hungarian nationals so often some resistance is demonstrated to the process of checking previous employments or academic qualifications. Formal written consent will always be required from candidates or employees going through a pre-employment screening process.</p> <p>In Hungary, the employer is responsible for ensuring that an individual has a right to work in the country.</p>
2.2	Major laws and regulations applying to pre-employment screening	<p>All legislation in Hungary has its origins in one of the articles in The Fundamental Law of Hungary which was revised in 2013.</p> <p>A new Labour Code was passed by the Hungarian government in December 2011. The code came into partial force in July 2012, taking full effect on 1 January 2013 after a six-month transition period. It replaced the Labour Code 1992, which was introduced immediately after the democratic transition from state socialism. The government expects that the law will make employment more flexible, cheaper and more market-compliant for employers and ultimately increase investment in Hungary.</p> <p>The Code lays down the fundamental rules for work in accordance with the principles of free enterprise and freedom of employment, taking into account the economic and social interests of employers and workers alike. It covers:</p> <ul style="list-style-type: none"> • employers • workers • employers’ interest groups • works councils and • trade unions.

The Code applies to user enterprises (Chapter XVI) and beneficiaries of services provided by school cooperatives (Chapter XVII). It also requires payment of a guarantee deposit for employees handling money or valuables. This precautionary deposit may be as high as one month's salary and is taken to allow the employer to cover possible losses. This should only be undertaken under legal advice.

Laws applicable to foreign nationals

Contracting parties can choose the governing law of the employment relationship in accordance with private international law. However, certain mandatory rules apply regardless of the choice of law. In particular if a European Economic Area (EEA) or non-EEA national employed by a foreign employer is posted to Hungary, Council Directive 96/71/EC concerning the posting of workers (Posted Workers Directive) applies. Under the Hungarian implementation of the Directive, the foreign employee is protected by the following mandatory rules under the Labour Code:

- maximum working time and minimum rest periods
- minimum annual paid leave
- minimum wages
- conditions for hiring-out workers
- occupational safety
- access to employment or work by:
 - pregnant women (or women who have recently given birth)
 - women with young children
 - young people, and
- the principle of equal treatment.

Act CXXV of 2003 on Equal Treatment (Equal Treatment Act) and the **Criminal Code (Act IV of 1978)** contain the main regulations against discrimination and harassment. The Equal Treatment Act lists grounds on which discrimination is prohibited:

- sex
- racial origin
- colour of skin
- nationality
- origin of national or ethnic minority
- mother tongue
- disability
- state of health
- religious or ideological conviction
- political or other opinion
- family status
- motherhood (pregnancy) or fatherhood
- sexual orientation
- sexual identity
- age
- social origin (that is, the employee's social background)

		<ul style="list-style-type: none"> • financial status • part-time or fixed-term employment or other type of work relationship • membership in an organisation representing employees' interests and • any other status, characteristic, feature or attribute. <p>A Penal Code came into force on 1 July 2013; it offers an effective response to the changes in crime patterns that have occurred in the 30 years since the Criminal Code came into effect.</p> <p>The National Authority for Data Protection and Freedom of Information is regulated by Act CXII of 2011 on Informational Self-determination and Freedom of Information (Privacy Act). The Act is comprehensive, and concerns all data control and data processing activities undertaken in Hungary. It defines these activities as those which relate to the data of a natural person, as well as data in the public interest and data made public on the grounds of being in the public interest.</p>
3	Pre-employment checks	
3.1	Identity check	<p>There are no sensitivities in undertaking identity checks in Hungary</p> <p>Official Hungarian identity documents are the Personal Identity Card (Személyazonosító Igazolvány), passport (Útlevel) and drivers' licence (Vezetői Engedély).</p> <p>A temporary passport would rarely be used for pre-employment screening since such a passport has to be handed in at the local notary's office (okmányiroda) or the Central Document Office (Központi Okmányiroda, 1133 Budapest, Visegrádi utca 110-112) after entry into Hungary. A full passport would have to be obtained after this.</p> <p>Marriage, birth or adoption certificates and tax notifications offer a lower level of identity verification and are not recognised as identity documents in their own right but can be used as supporting documentation.</p> <p>There is no known process for validating the authenticity of identity documents, passports or driving licences through the Hungarian government although commercial services exist through which checks can be carried out on their authenticity.</p> <p>The national ID card conforms to EU-wide standards.</p>
3.2	Checks on eligibility to work	<p>EU/EEA and Swiss citizens do not need to obtain a work permit for employment in Hungary. The employer must register its EU/EEA/Swiss employee at the local employment authority. Third-country nationals must obtain a work permit before the start of employment in Hungary. An individual work permit, for which the employee must apply, can be granted for a maximum of two years and may be renewed an unlimited number of times.</p> <p>There are exceptions from the work permit requirement (munkavállalási engedély) for executive and academic employees.</p>

		<p>Employers can recruit third-country nationals if they have advertised for specific positions, but were not able to fill their vacancies with Hungarian employees within the given timeframe.</p> <p>Obtaining permits</p> <p>Public employment services (Regionális Foglalkoztatási Szolgálat) and immigration offices (Bevándorlási Hivatal) in the future employer's region issue work and residence permits. The work permit is incidental to a residence permit.</p> <p>Cost</p> <p>Obtaining a work permit is free of charge but the employee bears the cost of official translations of the documents verifying his/her qualifications. EU/EEA nationals only pay the registration fee (HUF 1,500).</p> <p>In addition, third-country nationals must obtain a visa (€60) or a residence permit (HUF 18,000) depending on the length and scope of the employment.</p> <p>Turnaround</p> <p>The whole process (including obtaining work and residence permits) may take two to three weeks.</p>
3.3	Residency checks	<p>This check is often included as part of the Identity check as the individual's current address should be on the reverse side of their National ID Card.</p> <p>Alternatively, the employee may present to the employer an Address Registration Card, issued by the municipality in which he/she is resident.</p>
3.4	Criminal record checks	<p>Name of certificate</p> <p>Certificate of Good Conduct (Hatósági Erkölcsei Bizonyítvány).</p> <p>Department that holds records</p> <p>Criminal Records Authority, Central Office for Administrative and Electronic Public Services, 1097 Budapest, Vaskapu utca 30/A, Hungary.</p> <p>Where to apply within country</p> <p><i>By post</i></p> <p>Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala, Bűnügyi Nyilvántartó Hatóság, 1476 Budapest, Pf. 380, Hungary.</p>

In person

The Central Document Office,
1133 Budapest,
Visegrádi utca 110-112,
Hungary.

Website: www.nyilvantarto.hu/en/certificate_good_conduct

How to apply within country

By post

The individual must buy an envelope from the Hungarian Post Office, which contains an application form and a bank transfer slip. After completing the form and obtaining a receipt for payment, both must be sent to the address above.

In person

The certificate can be applied for at the address above.

Online

The application can be submitted online only if the applicant has access to the Client Gate (this can be requested from Hungary or a Hungarian Embassy).

For all methods of application the applicant must complete and sign the application form. The data provided is used as identification, which is carried out using the Population Register.

If the individual is applying in person they must show their ID card, driving licence or passport.

Who can apply

Individuals; third parties (with valid authorisation from the individual); and employers (in certain situations).

There are several professions, for which the law stipulates a special legal condition that must be fulfilled before taking the job. In those cases the future employee has to verify that the condition has been met by certificate.

Cost, payment and turnaround

The fee is HUF 3,100. If the certificate is applied for in person at the Central Document Office, the fee is HUF 4,400.

The applicant can pay the administrative service fee by:

- postal order or cheque attached to the application form
- bank transfer to the bank account of the Central Office for Administrative and Electronic Public Services or
- in person, by cheque or credit card.

The turnaround time is between 8 and 30 days. For applications in person, the turnaround time is five days, but certificates are usually issued immediately.

Further information can be obtained from the CPNI guidance on Overseas Criminal Record Checks which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.

<p>3.5</p>	<p>Education checks</p>	<p>Education checks are often required by employers to establish that a prospective employee has attended the educational establishments claimed.</p> <p>Typical information provided is dates of joining and leaving the educational institution (school, college or university), subject of study, courses (college, university), degree and final mark. In many cases, depending on the educational institution and its interpretation of the data protection legislation, this information will only be confirmed and not volunteered.</p> <p>A university may refuse at its own discretion to give any information even with written consent from the individual. Universities in Hungary often request a 'wet' signature consent form signed by the candidate and witnessed by two signatories.</p> <p>Furthermore, often questions regarding the character of an individual will not be answered by educational institutions in writing, although in some cases a verbal character reference might be obtained from a tutor or professor who knows the individual.</p> <p>Information covered by the Privacy Act cannot be obtained, except in circumstances where it is not considered potentially discriminatory.</p> <p>Applications for references must typically be made in writing and provide all known information, e.g. full name, date of birth, subject of study and give an explanation as to the reason for the request. However, whether any information will be disclosed or not depends on the university or college.</p> <p>Where the educational establishment is not well known, it may be necessary to undertake additional checks to verify its authenticity. In particular, employers should be alert to the risk of fake establishments and/or fake qualifications issued by such establishments.</p>
-------------------	--------------------------------	---

<p>3.6</p>	<p>Qualification checks</p>	<p>In Hungary verification of qualifications (academic or professional) is part of the pre- employment screening process for roles that require a particular qualification.</p> <p>Typical information provided is dates of joining and leaving the educational institution or professional body, membership status (professional body), and status and type of qualification. In many cases, all known information has to be provided. The institution will usually confirm this information although it might not volunteer any data.</p> <p>Generally questions regarding the character of an individual will not be answered by educational and professional institutions.</p> <p>Information covered by the Privacy Act cannot be obtained, except in circumstances where it is not considered potentially discriminatory.</p> <p>Application is made directly to the educational establishment or professional body concerned. Most educational establishments have standard processes for dealing with reference enquiries. The consent of the individual is generally required and recommended. Most professional bodies issue directories of members, so the accuracy of this type of information can be verified directly with the professional body. The information may sometimes be available on line for common qualifications.</p> <p>Fake documentation is widespread and it is regularly reported that a proportion of employment candidates lie or exaggerate about qualifications. For example, attendance at an educational establishment does not mean that the individual graduated from that establishment. It is also important to verify that an individual is an active member of a professional body and has not left nor been ejected from membership</p>
<p>3.7</p>	<p>Employment references</p>	<p>The Labour Book is commonly used by prospective employers as a means of validating their applicants' employment history.</p> <p>An individual's Labour Book will contain their social security number. Individuals may also wish to submit their Social Security card and tax card along with their Labour Book.</p> <p>Previous employers might still provide references if asked directly. These may confirm basic information such as dates of employment, positions held and reason for leaving. They will rarely include character references or personal comment.</p> <p>Many employers may refuse to provide character references and comments on performance, written or verbal, especially if they have issued a reference within the individual's Labour Book. Also, most employers will not provide information on salaries, sickness record or parental leave.</p>

		<p>Applications are generally made in writing to the employer concerned and a telephone call to introduce the request is often considered courteous in Hungarian culture.</p> <p>An employee must consent to the obtaining of such information, under data protection legislation.</p>
3.8	Financial/ credit checks	<p>Financial/credit checks are generally used only for very senior roles or those that involve access to financial systems or controls (in particular, in the banking and government sector). They are not commonly carried out outside the government or financial sectors and would be considered excessive in most other sectors.</p> <p>Financial or credit checks may be undertaken during the pre-employment screening stage, or on an ongoing basis more regularly where suspicions or concerns arise.</p> <p>In Hungary credit information relating to individuals and organisations is held in the Central Bank of Hungary. An individual may verify his or her own credit record directly with one of the main credit referencing agencies in Hungary. A third party may access information on an individual, with the express, prior, written consent of that individual.</p>
3.9	Substance abuse screening	<p>There is no specific legislation on workplace drug testing. Alcohol and drug testing at work is a controversial topic in Hungary. In certain occupations, companies and sectors where safety concerns are high, there may be a need to guarantee that workers do not work under the influence of alcohol or other psychotropic substances in order to avoid risks to themselves, fellow workers and other people, or even the production process itself (including machinery, technological devices, raw materials or final products).</p> <p>The Act on Labour Safety (No. 93/1993) does not authorise labour safety controllers to carry out drug tests. The practice of the courts is only standard in the field of alcohol tests: where agreed by workplace representatives, involvement is obligatory for all employees.</p> <p>A 2005 Resolution on workplace drug tests by the Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information states:</p> <ul style="list-style-type: none"> • employees may not be asked to give voluntary consent because of the inequality of power • tests might lead to a practice that violates privacy and • the efficacy of generally available mobile tests is not convincing.

3.10	Occupational health checks	<p>Employers in Hungary must provide occupational healthcare for their employees to comply with the Labour Safety Act and sectoral decrees.</p> <p>Participation in a pre-employment medical examination is compulsory for everybody and the examinations must be repeated regularly; annually or bi-yearly, depending on the position of the given employee.</p> <p>The occupational medical check is a thorough physical examination; it includes a variety of tests that ensure that any potential problems will be picked up, allowing the individual to take steps either to prevent them or begin early treatment.</p> <p>Health records must not be kept as part of personnel files, but stored separately by the occupational medical doctor. No one else will have access to them.</p>
4 Personnel security measures during employment		
4.1	Legal requirements	<p>The European Convention on Human Rights applies to all EU countries.</p> <p>Organisations should bear in mind the importance of several Articles within the Convention, such as:</p> <ul style="list-style-type: none"> • Article 5, which protects an individual from unlawful arrest or detention • Article 8, the right to private and family life; organisations conducting an investigation that may involve the collection of information relating to an employee’s private life should ensure that any resulting infringement of the right to privacy can be justified, which means that the amount and extent of evidence collected should be both necessary and proportionate in the context of the type of investigation being carried out and the nature of the incident or suspicion and • Article 14; employers should not take actions that could be seen as discriminatory or persecutory under the Convention. <p>Act CXII of 2011 (Privacy Act) on Informational Self-determination and Freedom of Information (see Section 2.2).</p> <p>Act CXXXIII 2005 regulates the following types of activity:</p> <ul style="list-style-type: none"> • personal and property protection activities • security system design and installation activities (‘designer mounting activity’) and • private detective activity. <p>The Act states:</p> <p>(2) For the purposes of this Act, personal and property protection activities [are]:</p> <ol style="list-style-type: none"> a) protecting the lives and physical integrity of individuals, b) guarding property or chattels c) accompanying the transportation or consignment of cash and valuables

		<p>d) event security and e) in a) to d) organisation and management activities in points.</p> <p>(3) Personal and property protection activities carried out by a person who has any of the following qualifications:</p> <p>a) security guard b) bodyguard c) guard or d) security organisation.</p> <p>All of the above activities may also be carried out using technical security systems and auxiliary devices. Protection with the help of technical security systems means surveillance and control of guarded facilities by technical means and checking the signals obtained.</p> <p>Under the Labour Code, employees who believe they have been dismissed unfairly can complain to a tribunal.</p> <p>The Labour Safety Act details health and safety requirements for work organisations, as well as requirements for preventing work accidents and employment-related illness.</p> <p>The Labour Safety and Labour Management Directorate, as well as the labour safety and labour management special administrative bodies of the Budapest and county government offices, and labour safety and labour management inspectorates, are responsible for public administrative duties relating to labour safety and the activities of labour authorities.</p> <p>The influence of trade unions in Hungary has steadily been declining with a fall of 11% recorded in 2011. There are a few core union confederations remaining that impose a collective influence on employers:</p> <ul style="list-style-type: none"> • the Democratic League of Independent Trade Unions (LIGA) • the Autonomous Trade Unions Confederation (ASZSZ) • the Confederation of Unions of Professionals (ÉSZT) • the Forum for the Cooperation of Trade Unions (SZEF) • the National Federation of Workers' Council (Munkástanácsok) and • the National Confederation of Hungarian Trade Unions (MSZOSZ).
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	<p>The employer may be protected by some intellectual property rights (including libel, slander and trademark law), and rights imposed under the employment contract. Legal action for breach of contract may restrain an employee from dealing in client-confidential information; however it is unlikely to deter more serious offences without the imposition of other controls (such as physical access or monitoring controls, etc).</p>

4.4	Local legislation that specifically governs the rights of the employee	As outlined above, legislation governs the rights of an employee. This may restrict the level of self-protection permissible. However, under the data privacy laws in Hungary, the gathering and processing of personal data is permissible, if the legitimate interests of the personal data administrator (the employer) are not overridden by the interests of the individual (the employee) to whom such data relate. All processing must be justifiable and reasonable and not infringe on the individual's fundamental rights under the European Convention on Human Rights.
4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	Individuals may bring claims against their employer under the legislation set out above.
4.6	What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?	<p>A claim for unfair dismissal may be brought under one of the explicitly specified preconditions in the Labour Code. Furthermore, under the Privacy Act, a complaint for breach of an employee's rights may be submitted by the injured party to the National Authority for Data Protection and Freedom of Information, which may impose requirements and sanctions on the employer. Beside the complaint to the Commission, under the Privacy Act the employee whose rights have been breached is entitled to file a claim before the courts.</p> <p>There is an official Labour Court system in operation in Hungary.</p> <p>The principal jurisdictions of the Labour Courts concern:</p> <ul style="list-style-type: none"> • violation of labour contracts • unfair dismissal • discrimination claims • violation of the rest periods rules • wages disputes • disciplinary decisions • employers/employees' liability decisions and • administrative overview of social secure and labour supervisors' decisions. <p>There are no qualifying periods before claims of unfair dismissal may be brought. Under the Labour Code (ss 89 and 96) the rules for dismissal are:</p> <p>Section 89:</p> <ol style="list-style-type: none"> 1. Both the employee and the employer may terminate the employment relationship established for an unfixed term by notice. No deviation from this provision shall be considered valid. 2. Employers must justify dismissals, clearly indicating the cause. In a dispute, the employer must prove the authenticity and substance of the reason for dismissal.

		<p>3. An employee may be dismissed only for reasons in connection with ability, behaviour in relation to the employment relationship or with aspects of the employer’s operations.</p> <p>4. A change of employer by legal succession may not serve in itself as grounds for termination by ordinary dismissal of an unfixed-term employment relationship.</p> <p>5. Prior to dismissal by the employer on grounds of work performance or conduct, an opportunity must be given to the employee to defend him/herself against the complaints raised, unless this is unreasonable in view of all the applicable circumstances.</p> <p>Section 96:</p> <p>1. An employer or employee may terminate an employment relationship by extraordinary dismissal if the other party</p> <p>a) wilfully or by gross negligence commits a grave violation of any substantive obligations arising from the employment relationship, or</p> <p>b) otherwise engages in conduct rendering further existence of the employment relationship impossible. No deviation from this provision shall be considered valid.</p> <p>2. Section 89(2) will apply to extraordinary dismissals. Prior to the employer’s announcement of extraordinary dismissal the employee must be told the reasons for the planned action and to defend him/herself against the complaints raised, unless this is unreasonable in view of all the applicable circumstances.</p> <p>3. Cases in which the legal consequences in 1. apply may be stated in the collective bargaining agreement or employment contract.</p> <p>Failure to follow the statutory procedures by the employer prior to dismissal will render that dismissal automatically unfair. The employee is entitled to claim to be restored to his/her position and to claim compensation for unfair dismissal against the employer.</p>
4.7	<p>Availability of security measures</p>	<p>Restriction of access to premises</p> <p>No specific restrictions exist.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>No specific restrictions exist as long as the employer is not preventing the employee from carrying out his/her specific duties as a result.</p> <p>Physical screening (on entry/exit)</p> <p>No specific restrictions exist although culturally this would be viewed unfavourably without probable cause or suspicion of criminal activity. It would be considered more acceptable on highly secure and government sites.</p>

Prohibition of removal of data from the premises (hard-copy)

The Data Privacy Act (DPA) governs protection of personal data. Removal of data from the premises or from secure systems may constitute a breach of the DPA if it involves other data subjects i.e. information on customers or members of the public.

Employers are also covered under the protection of industrial properties in Hungary.

The basic framework for this protection is the Act on Invention Patents. The Civil Code and the Competition Act protect also unpatented inventions. There are separate laws to protect utility models, designs, trademark indicators and geographical indicators. The Civil Code also helps to protect economic, technical and organisational knowledge and experiences that have a material value ('know-how').

Prohibition of removal of data from the premises (electronic)

See above.

Visual surveillance (CCTV or other cameras), either overt or covert

The Labour Code does not contain detailed provisions applicable to electronic surveillance devices, such as CCTV. Provisions relating to these devices are contained in the Personal and Property Protection Act (Act CXXXIII of 2005), which also establishes the lawful grounds for the use of electronic surveillance systems and obligatory retention periods. Although the rules of the Personal and Property Protection Act do not cover all aspects of electronic surveillance, the agency responsible for its administration will take the act's provisions into consideration until the Labour Code's provisions are adequately amended.

Employers are obliged to prove that their electronic surveillance systems comply with the requirements of the Privacy Act and in particular that the processing is for a lawful purpose. CCTV surveillance must not jeopardise human dignity; accordingly, cameras may not be directed at a particular employee nor record his/her activity alone. Furthermore, an electronic surveillance system will be deemed unlawful if it is aimed at influencing employee behaviour in the workplace. CCTV surveillance is not allowed in locker rooms, showers, toilets, medical rooms and similar premises, nor in rooms or locations where employees spend their breaks. However, these locations can be lawfully monitored after working hours when not in use by employees.

A camera must only aim at the designated area and only at the premises of the employer. An employer must precisely set out in its policy the purpose of installing every camera and the reason for monitoring each area. It will not be enough for employers to provide employees with general information on electronic surveillance systems.

The general maximum retention period for personal data collected by electronic surveillance systems is three days. In exceptional cases, longer retention periods can be applied, but only if the employer is able to justify that special circumstances require a longer retention period. Only a limited number of staff may have access to personal data, and employers must also set out rules of access to data.

Overt monitoring of access to IT and other equipment

Under the Labour Code, an employer is entitled to monitor employment-related behaviour of its employees, something which certainly entails the processing of certain personal data. The Labour Code does not state that the employer is obliged to obtain consent from the employee, and reliance on employee consent may not be valid: as set out in Opinion No 15/2011 of the Article 29 Working Party, grounds other than consent are contained in Article 7 of the EU DP Directive that can be used as a lawful basis for data processing.

Employee monitoring does not necessarily require employee consent, but certain requirements must be met:

- employee monitoring is only deemed lawful if it is essential for a purpose directly related to the aim of the employment
- the human dignity of the employee must be respected and his or her private life must not be monitored
- employees must be informed in advance about the data processing, and
- the employer must comply with the general principles set out in the Privacy Act, including the requirement of a fair and lawful purpose for data processing.

The Labour Code provides a framework for lawful employee monitoring, but in any event, details of monitoring must be set out in a separate policy and the monitoring must comply with principles of accountability and proportionality.

Covert monitoring of access to IT and other equipment

Where monitoring involves the collection of personal data, the DPA requires that such data is collected lawfully and processed in a fair and proper way.

Reporting hotlines (anonymous)

Personal data must be handled in accordance with the DPA.

Reporting hotlines (confidential)

Personal data must be handled in accordance with the DPA.

		<p>Use of alerts/automated warning systems to identify unusual employee behaviour (out of hours activities, duplicate payments)</p> <p>The use of automated warning systems is not specifically regulated by law or regulation. The employer should assess the need for such a system based on the overriding requirements of the data protection legislation to demonstrate a proportionate response to risks. Any systems implemented must not place the employer in breach of the Labour Code.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>Where monitoring involves the collection of personal data, the DPA requires that such data are collected lawfully and processed in a fair and proper way.</p>
4.8	Formal investigations	<p>Is there a licensing regime covering investigators?</p> <p>Act CXXXIII 2005 governs private investigator activity.</p> <p>Physical surveillance (overt or covert)</p> <p>Physical surveillance is covered by the Fundamental Laws, the European Convention on Human Rights and Act CXXXIII 2005.</p> <p>Act CXXXIII 2005 does not provide detail about the application of physical surveillance.</p> <p>Electronic surveillance (e.g. tracking devices)</p> <p>See ‘Physical surveillance’ above.</p> <p>Visual and communication surveillance (using cameras, video or CCTV)</p> <p>Governance of the use of video surveillance for employees is outlined under the Labour Code. (See Section 4.7)</p> <p>Communication intercept (including oral, written and electronic communication including bugging devices)</p> <p>The use of communication intercept is subject to the Fundamental Laws, the European Convention on Human Rights and Act CXXXIII 2005.</p> <p>Computer or database surveillance (using either hardware or software tools, including forensic tools)</p> <p>The use of communication intercept is subject to the Fundamental Laws, the European Convention on Human Rights and Act CXXXIII 2005.</p> <p>Formal interviews of staff</p> <p>The conduct of formal interviews is permissible, subject to the overriding requirements relating to respect of an individual’s rights as set out in the Fundamental Laws and the European Convention on Human Rights.</p>

		<p>Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)</p> <p>See above. In addition, an employer should take into account the requirements of the DPA.</p> <p>Search and seizure of evidence, whether electronic or physical (overt or covert)</p> <p>Act CXXXIII 2005 governs the seizure of evidence by security professionals. Employers should take any action into consideration under the Fundamental Laws, the European Convention on Human Rights and the DPA.</p> <p>Is it either usual or necessary to involve the police in investigations?</p> <p>It is not believed to be necessary to involve the police in each case of surveillance and safeguarding although for criminal matters it is important to involve them, even if the surveillance is being handled internally.</p> <p>If the police are involved, at what stage in the investigation does this generally occur?</p> <p>The decision as to when and if to involve the police may depend on a number of factors such as the severity of the matter; the speed of response required (the police might not have adequate resources); access of the organisation itself to investigation capability (typically, small organisations may be less able to respond to an incident than a large organisation with pre-defined resources and processes). In any case when there is data on a committed violation of public order or a crime the police should be notified immediately.</p> <p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>In Hungary as in the UK, the police have limited resources and therefore cannot realistically investigate all cases in detail. An organisation may undertake its own investigation, alone or in conjunction with a third party, provided that all activities comply with the applicable Hungarian legislation as outlined above.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>Suspected violations of public order or criminal activities should be reported to the police immediately.</p> <p>Breaches of regulatory conduct within financial services organisations must be reported to the appropriate regulator.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

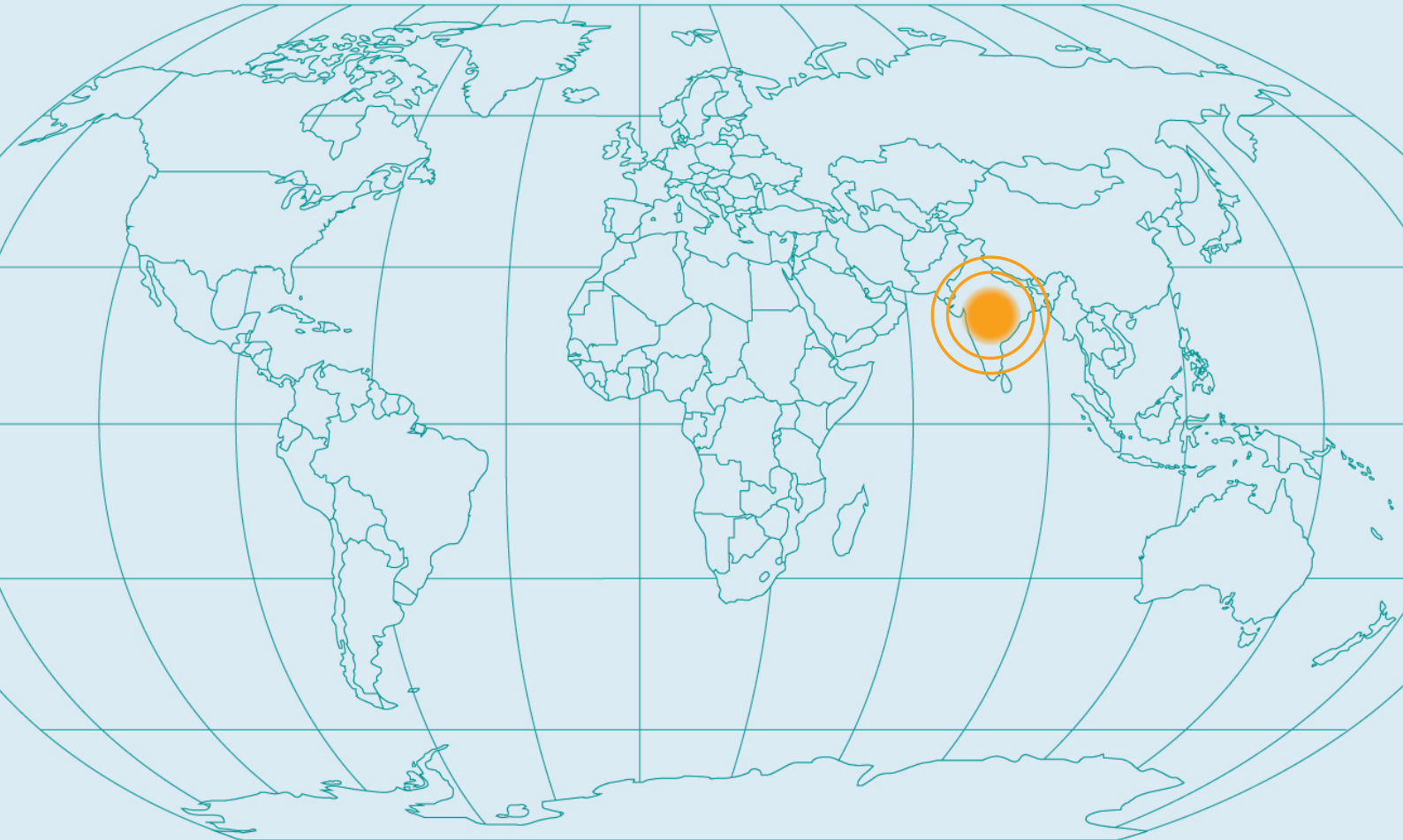
CPNI

Centre for the Protection
of National Infrastructure

SECURITY **WATCHDOG**
Part of Capita plc

India

Personnel Security in Offshore Centres



India

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1	Introduction	<p>India is the largest offshoring location for companies in the world. A significant number of international organisations have operations based in India, particularly in the financial services, information technology (IT), pharmaceutical and IT-enabled services (ITeS)/business process outsourcing (BPO) sectors. These organisations typically employ stringent pre-employment security screening and ongoing security screening of employees. Local employers may also undertake pre-employment screening measures, albeit less extensively than international organisations.</p> <p>In India employers are not generally restricted by law/regulation from undertaking measures that are proportionate to the risks posed by employees. There are a number of laws that protect the rights of an employer, particularly in relation to its data or property. In addition, the employment contract of each organisation – known as the <i>Code of Business Conduct</i> – stipulates the rights and obligations of the employee and the employer (see Section 2.2). Provided that the employer acts within the law, it can impose restrictions and/or conditions on employees to protect its interests. If employees act in disregard of the Code of Business Conduct they cannot subsequently claim victimisation by the employer.</p> <p>There are some practical limitations on employers undertaking pre-employment security screening. For example, there is no centralised system for conducting criminal record checks, and the system relies largely on manual processes. Credit or financial checks are not generally undertaken as part of the pre-employment process, except for those categories of employment requiring access to sensitive data or systems (such as in financial institutions). In addition, third-party sources of information (such as electoral data and telephone subscriber data) are not complete or necessarily up-to-date. This may necessitate a higher degree of manual intervention to verify the accuracy or completeness of information provided by prospective employees.</p>
2	Personnel security measures during recruitment	
2.1	Culture of screening	<p>Pre-employment screening measures are regularly used by companies in India. It is normal practice to verify information including previous employment history, education credentials, criminal record data and residency data. Further checks are also regularly undertaken against published regulatory and compliance lists, such as the Specially Designated Nationals list published by the US Treasury Department Office of Foreign Assets Control.</p> <p>The level of pre-employment screening is generally commensurate to the role and responsibilities of the individual concerned. For example, an individual with access to sensitive financial data would generally be subject to greater levels of screening than one who did not have such access.</p>

		<p>In international companies, employees are generally vetted to a higher level than in domestic companies and this may match the level of screening carried out in their respective home countries. Increasingly companies have begun to screen all employees, although this is not yet an industry-wide practice.</p> <p>In India it is common practice for organisations to outsource their pre-employment screening to third-party service providers who will contact previous employers to validate employment history, educational institutes for educational qualifications and police authorities for criminal records. Owing to the lack of reliable third-party data sources, residency data is usually verified through physical site visits. It is also notable that, in India, representations are often made verbally and not in writing.</p>
2.2	<p>Major laws and regulations applying to pre-employment screening</p>	<p>The major laws applying to pre-employment security screening are as follows:</p> <ul style="list-style-type: none"> • The Child Labour (Prohibition and Regulation) Act, 1986 prohibits the employment in certain occupations and processes of children who have not reached 14 years of age. • The Contract Labour (Regulation and Abolition) Act, 1970 prohibits the employment of contract labour in jobs of a perennial nature. • The Equal Remuneration Act, 1976 requires equal remuneration to be paid to male and female workers and prevents discrimination on the ground of sex against women in the context of their employment. • The Minimum Wages Act, 1948 provides for minimum rates of wages to be fixed in certain employments. • The Foreigners (Amendment) Act, 1946 relates to rights of residency and employment in India. Contravention of the Act is punishable by imprisonment for of up to five years, a fine and expulsion from the country. • The Information Technology (Amendment) Act 2008 (IT Amendment Act 2008) relates, amongst other issues, to the protection of sensitive personal data and security practices and procedures that must be followed by organisations dealing with such data (Data Privacy Rules). • The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the 'Privacy Rules') have recently introduced new and more stringent rules with regard to the processing and security of personal data. Employers should be aware that these rules are more restrictive than the equivalent EU or US legislation. For example, in order to collect and use 'sensitive data' employers, without exception, must first obtain the written consent of the subject.

		<p>Code of Business Conduct and Certified Standing Orders</p> <p>The Code of Business Conduct (or Employee Handbook, Employee Manual, Employee Standard Operating Procedure, etc) is a formal document with defined contents and categories. It defines what constitutes ‘misconduct’, as well as procedure and provisions for disciplinary action and redress of grievances.</p> <p>Each organisation defined as an ‘industrial establishment’ is obliged by law under the Industrial Employment Standing Orders Act, 1946 to have Standing Orders certified under the Act. Those establishments that are not covered by the Act will have a Code of Business Conduct that is an extension of the appointment letter (setting out terms and conditions) governing the employee. This is given to the employee at the time of their appointment and sets out the organisation’s codes of practice.</p> <p>Certified Standing Orders, which are applicable to ‘industrial establishments’, must be certified by the Certifying Officer notified under the Industrial Employment Standing Orders Act, 1946 and constitute the general terms and conditions relating to employment, rules, leave, discipline, grievance handling, age of retirement, etc.</p> <p>The difference between Certified Standing Orders and the Code of Business Conduct is that the Code is accepted by the individual employee and any dispute or differences arising can be resolved by civil courts. In contrast, there is a formal procedure for resolution of disputes under Certified Standing Orders as governed by the Industrial Disputes Act. This may involve referral to a Labour Court, the outcome of which is binding on both parties.</p>
3	Pre-employment checks	
3.1	Identity check	<p>There are no national ID cards issued in India that can be readily verified.</p> <p>Most Indians will hold one or more of the following types of identification:</p> <ul style="list-style-type: none"> • a driving licence issued by the state government • voter’s ID issued by the state government • a passport: only Indians who intend to travel overseas would apply for a passport and this is issued by the Government of India after stringent verification by the police authorities; passports contain machine-readable security features or • a Permanent Account Number (PAN) card issued by the Income Tax Authority of India: any individual whose income for the full financial year exceeds a threshold for taxable income must file an income tax return, which cannot be accepted by the income tax authority without a PAN number. <p>In exceptional circumstances, a certificate of identity could be provided by a person of standing in the community (e.g. a doctor, solicitor or local government official).</p>

3.2	Checks on eligibility to work	<p>Employers must obtain permission to employ a foreign national (in the form of a work permit or visa) and it is therefore a standard pre-employment step to approach the local special branch of the police.</p> <p>An employment visa/work permit is issued to a foreign national by overseas Indian embassies/high commissions, prior to his or her arrival in India. It is granted on presentation of a letter of invitation issued by the hiring company. Foreign nationals must register with the Foreigner’s Regional Registration Office (FRRO) within 14 days of arrival in India. The FRRO is responsible for maintaining records of all foreigners entering/leaving the country.</p> <p>For verification purposes, the prospective employer may take a photocopy of the employment visa/work permit and write to the FRRO to verify its authenticity.</p> <p>Further information and contact details can be found at http://froidia.com/.</p>
3.3	Residency checks	<p>It is common practice in India to undertake checks on current and former addresses of a prospective employee.</p> <p>This information is usually accessed by the employer or an appointed third party on behalf of prospective employees.</p> <p>Voter ID, PAN cards, passports, ration cards, rent agreements, driving licences or utility bills payable to the Corporation of India are commonly used sources of residency information.</p> <p>Because in India voters’ roll information and telephone subscriber information is unreliable, ideally residency information will be verified by physically visiting the address. This may not be possible for more remote addresses.</p>
3.4	Criminal record checks	<p>Name of certificate</p> <p>Local Police Certificate (also known as Police Clearance Certificate or Character Verification Record).</p> <p>Department that holds records</p> <p>The National Crime Records Bureau (NCRB), East Block-7, R.K. Puram, New Delhi-110066, India.</p> <p>Telephone: +91 (0) 11 26172324/ +91 (0) 11 26105353 Fax: +91 (0) 11 26186576/ +91 (0) 11 26197984 Email: comm@ncrb.nic.in</p> <p>Where to apply within country</p> <p>Through a local Indian police station (no contact details available) or a Regional Passport Office, details of which can be found at: www.passportindia.gov.in/AppOnlineProject/welcomeLink</p>

How to apply within country

Applications via the local police station

Application forms are obtained from the local police station.

An individual must complete the application form and include the following:

- a passport-sized photograph
- a certified copy of their passport, driver's licence, voter's identification card, PAN card or ration card
- current address
- previous address and other residential history covering a ten-year period
- name and date of birth of the individual's father and
- proof of payment.

For employment purposes, a prospective employer is required to submit an application form that has been completed and signed by the individual. The form must be accompanied by a covering letter typed on company letterhead. The letter must be signed by an authorised signatory.

It is advisable for authorised company personnel to visit the police station to follow up approximately seven days after an application has been made.

Applications via the Regional Passport Office

Individuals may submit an application for criminal records disclosure via the Regional Passport Office.

The same application process applies as for applications via the local police station.

The Regional Passport Office will verify the information with the local police station.

Prospective UK employers cannot use this route to submit a request for criminal records disclosure on behalf of an individual.

Who can apply

Individuals or employers (with consent).

Cost, payment and turnaround

Cost

Within India, there is no standard fee and cost varies between INR10 and INR3,000.

Payment

Methods of payment vary between police stations, but payment is usually by a bank draft or postal order.

		<p>Turnaround</p> <p>The certificate can be collected in person from the local police station within seven to ten working days.</p> <p>Individuals can request that the Indian Police Service send results by post, which can take up to 30 working days.</p> <p>There is a fast-track system in place for the disclosure of priority cases. However, there is no specific timeframe for fast-track requests.</p> <p>Legislation</p> <p>Indian Penal Code 1860.</p> <p>Further information can be obtained from the CPNI guidance on Overseas Criminal Record Checks which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>
3.5	Education checks	<p>In India education checks are routinely undertaken to verify attendance at educational establishment(s) and dates of study.</p> <p>Such checks generally require original documents to be presented by the potential employee including:</p> <ul style="list-style-type: none"> • Secondary School Certificate, i.e. Class 10 (issued by the Central Board of Secondary Education on clearing the All-India Secondary School Examination) • Higher Secondary School Certificate, i.e. Class 10+2 (issued by the same Board on the same occasion) – both these documents are also accepted as proof of age/date of birth, and • University Certificate/degree issued by a college/university or by the Board of Education, Government of India.
3.6	Qualification checks	<p>Verification of qualifications (academic or professional) is a regular part of pre-employment screening in India.</p> <p>Typical information provided is:</p> <ul style="list-style-type: none"> • dates for joining and leaving the educational institution or professional body or • membership status, status and type of qualification (professional body). <p>In many cases, all known information has to be provided. The institution concerned will confirm this information.</p> <p>Generally, questions regarding the character of an individual will not be answered by educational institutions in writing, although in some cases a verbal character reference might be obtained from a tutor or professor who knows the individual.</p> <p>Details may be confirmed directly with the educational establishment or the professional body. Most educational establishments have standard processes for dealing with reference enquiries. The consent of the individual is generally required.</p>

<p>3.6</p>	<p>Qualification checks</p>	<p>Most professional bodies issue directories of members, so the accuracy of this information can be verified directly with the professional body. The information may be verified online, by telephone or via written communication. It is important to verify that the individual is an active member of a professional body and has not left nor been ejected from membership.</p> <p>Fake documentation is widespread and it is reported that a large proportion of employment candidates exaggerate or lie about their qualifications.</p> <p>To mitigate the risk of fake documentation, an employer may take the following steps:</p> <ul style="list-style-type: none"> • require original documentation to be presented (for example, the Class 10, Class 10+2, college/degree certificate or postgraduate degree/certificate) • write to the educational/professional establishment concerned attaching a photocopy of the relevant documents to verify their authenticity or • thoroughly check the documents provided by the prospective candidate against the application form for any disparities, or gaps in information.
<p>3.7</p>	<p>Employment references</p>	<p>It is normal for employers to provide references. These may confirm basic information such as dates of employment, positions held and reason for leaving. They will not necessarily include character references. Candidates may also provide a 'relieving letter' issued by a previous employer upon leaving employment. The 'relieving letter' (which may also be referred to as an 'experience certificate') typically certifies:</p> <ul style="list-style-type: none"> • duration of employment • nature of employment • last held designation • last salary drawn • reason for leaving and • character/integrity. <p>Verification is generally undertaken by an application made directly to the Human Resources (HR) department of the former employer. In India most employers retain employment data for at least five years.</p> <p>Some common issues experienced in India include the use of fake certificates and fake salary slips.</p> <p>Where the employer is not well known, it may be necessary to undertake additional checks to verify its existence/background.</p> <p>Character references from previous employers</p> <p>This option is available to prospective employers in India, but is not common practice. Character references are more commonly obtained from persons of standing in the community (see below).</p> <p>Application would be made directly to the HR department of the previous employer, or to a named previous supervisor of the prospective employee.</p>

		<p>Character references from persons of standing in the community</p> <p>Typically, character references may be sought from persons of standing in the community such as police officers or professionals. These individuals will typically have known the individual for a period of time (e.g. more than three years).</p> <p>Information may be sought directly from nominated individuals. In India candidates are known to commonly name friends as referees, so caution should be exercised when taking up such references.</p>
3.8	Financial/ credit checks	<p>It is not common practice in India to request data on the creditworthiness of a prospective employee. However, where the position applied for is of a potentially sensitive nature, the organisation’s Code of Business Conduct may contain clauses requiring screening for financial or credit issues as part of the ongoing personnel security regime. It would then be mandatory for the relevant employee to reveal information voluntarily or be faced with a Code violation.</p> <p>Credit or account information cannot be accessed from banks and other financial institutions without the written consent of the individual.</p> <p>CIBIL (Credit Information Bureau (India) Ltd at www.cibil.com/) is the national body that provides credit and financial data. However, the credit history of an individual is not available for employment purposes.</p>
3.9	Substance abuse screening	<p>Screening for substance abuse is not yet widespread in India as part of the pre-employment screening process.</p> <p>Explicit consent of the individual would be required to conduct such screening.</p> <p>The candidate is normally required to visit a designated medical centre to provide screening samples such as blood or urine. Candidates are required to carry a form of identity when attending these tests.</p> <p>To eliminate any problems of fake ID/tests, the pre-employment medical check-up is normally instigated and paid for by the hiring organisation using a trusted and recognised medical centre/hospital. It is good practice for the hiring organisation to define the kind of tests/ screening that must be undertaken; these might include:</p> <ul style="list-style-type: none"> • substance abuse risk • any physical/chronic ailment that might hinder discharge of duties • ECG, treadmill, blood-pressure, blood and urine tests and • chest X-rays. <p>There is no legal restriction prohibiting the employer from asking the prospective employee to undertake these tests. However, it is good practice to obtain consent to a medical examination in the employment application form.</p> <p>It is accepted practice that the issuance of an appointment letter is subject to the employee’s medical fitness as defined by the employer.</p>

3.10	Occupational health checks	Occupational health checks are not common practice in India. They are restricted to certain specific sectors, mainly government services. Explicit consent of the individual would be required to conduct occupational health checks. (see Section 3.9).
4 Personnel security measures during employment		
4.1	Legal requirements	<p>In India, there are approximately 67 national legislative acts, in addition to many other state laws, governing and regulating the rights of employees and employers. These include:</p> <ul style="list-style-type: none"> • the Child Labour Act • the Contract Labour (Regulation and Abolition) Act • the Dangerous Machines Act • the Employers’ Liability Act • the Factories Act, 1948 • the Industrial Disputes Act, 1947 • the Minimum Wages Act • the Trade Unions Act, 1926 • the Industrial Employment Standing Orders Act, 1946 and • the Workmen’s Compensation Act. <p>Within outsourcing organisations in India, it is an accepted practice for employers to impose stringent measures to protect privacy. Employees will often enter into a legally binding contract at the time of joining in which they are obliged to be:</p> <ul style="list-style-type: none"> • checked on entry/exit • barred from access to certain areas in the premises and from certain information • limited in access to the internet and • limited in the use of electronic media for data transfer, etc. <p>The Information Technology Act, 2000 provides legal recognition for transactions carried out by electronic data interchange and other means of electronic communication, commonly referred to as ‘electronic commerce’, which involve the use of alternatives to paper-based communication and storage of information and facilitate electronic filing of documents with government agencies.</p> <p>The Private Security Agencies (Regulation) Act, 2005 regulates private investigators in India.</p>
4.2 Laws governing the rights of the employee or employer		
4.3	Local legislation that specifically governs the rights of the employer	<p>India has enacted several pieces of legislation to meet the obligations imposed on it by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), a World Trade Organization agreement. See</p> <p>www.wto.org/english/tratop_e/TRIPS_e/TRIPS_e.htm</p>

		<ul style="list-style-type: none"> • The Trade and Merchandise Marks Act, 1958 has been replaced by the Trademarks Act, 1999 • the Copyright Act, 1957 has been amended to protect computer programs as literary work • the Patent Act, 1970 has been amended by the Amendment Acts of 1999 and 2002 and • the Designs Act of 2000 has completely replaced the Designs Act of 1911. <p>Intellectual property rights are constantly evolving and are now contained within a number of separate pieces of legislation. These include patents, copyright, trademarks, trade secrets and registered design, among other rights.</p> <p>In addition, most of the Acts that apply to industrial establishments specifically govern and regulate the rights of employers. For example, the Industrial Disputes Act, 1947, the Factories Act, 1948, the Shops and Establishment Act, etc. Other legislation, such as the Indian Penal Code, 1860, the Criminal Procedure Code and the Information Technology Act, 2000, governs and regulates the rights of the employer.</p>
4.4	Local legislation that specifically governs the rights of the employee	Both registered and recognised trade unions exist in India. Their activities are governed by the Trade Unions Act, 1926. Under this Act, any seven members can form a union and have it registered. A union may be registered but the employer does not have to recognise it. Recognition comes when the employer enters into collective bargaining with the union. In any one organisation there may be more than one union, but the employer will deal only with the union that is followed by the majority of workers.
4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	<p>Where employees are governed by a Code of Business Conduct or Certified Standing Orders (as applicable) they cannot challenge the employer's use of security procedures in the courts. Even if they bring a challenge before the Labour Court/a civil court they are unlikely to obtain relief.</p> <p>Under the Information Act, 2000, an employer may protect its premises and information.</p>

<p>4.6</p>	<p>What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?</p>	<p>Employee grievances are handled by the employer through the HR department (e.g. the welfare officer in a factory) and collective bargaining through any recognised trade union. For resolution of disputes, options are set out under the Industrial Disputes Act, 1947, including conciliation, Labour Courts and industrial tribunals, etc.</p> <p>'Grievance handling' and its procedure are also provided under the Industrial Employment Standing Orders Act, 1946 and the Certified Standing Order applicable in the factory. In addition, an employee is governed by the Code of Business Conduct that he/she signed and accepted at the time of joining the organisation and any violations of the Code warrant serious action against the employee. The Code of Business Conduct is an important document that safeguards the interests of both the employer and the employee. The employee cannot be deemed to be victimised if he or she does not adhere to the grievance-handling process laid down in the Code of Business Conduct. This is particularly relevant in sectors such as outsourcing, IT, ITES, etc.</p> <p>The disciplinary process applies specifically to the 'workman' category as set out under s. 2(S) of the Industrial Disputes Act, 1947 (amended 2009). It covers any person employed to undertake any manual, unskilled, skilled, technical, operational, clerical or supervisory work. It does not include persons who are employed mainly in a managerial or administrative capacity, nor those employed in a supervisory capacity drawing a salary of more than INR 10,000 per month.</p> <p>For persons who come under the definition of 'workman' the disciplinary process is:</p> <ul style="list-style-type: none"> • incident • preliminary investigation • complaint • charge sheet • written explanation • ordering an internal enquiry • conducting internal enquiry • independent or contested enquiry • recording proceedings • collection of evidence • report of the enquiry officer • show cause notice and • disciplinary action. <p>For persons who do not come under the definition of 'workman' the only remedial action available is to approach the civil court for enforcement of the terms and conditions of their employment contract and the Code of Business Conduct.</p>
-------------------	---	--

<p>4.7</p>	<p>Availability of security measures</p>	<p>Restriction of access to the premises</p> <p>Such measures are legal and binding under the Information Technology Act, 2000, the Code of Business Conduct and Certified Standing Orders. Premise protection measures are socially accepted in India and are considered a right of the employer. The employer’s rights are supported by law. Access rights are stringently enforced, particularly by outsourced/offshored operations.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>See above.</p> <p>Physical screening (on entry/exit)</p> <p>See above.</p> <p>Prohibition of removal of data from the premises (hard-copy)</p> <p>Under the provisions of the Information Technology Act, 2000, reinforced by the Code of Business Conduct, the employee is prohibited from removing any sensitive/vital company information on paper or by electronic data transfer. It is also common practice for employers to prohibit employees from bringing pen drives, compact discs, personal camera cellphones, laptops, etc onto their premises.</p> <p>Prohibition of removal of data from the premises (electronic)</p> <p>See above.</p> <p>Visual surveillance (CCTV or other cameras), either overt or covert</p> <p>This is covered under the Code of Business Conduct and is a legitimate right of the employer to protect its property while the employee or visitor is on its premises. Thus overt or covert CCTV surveillance in the workplace is accepted and practised on condition that there should be no surveillance in changing rooms, rest rooms and toilets.</p> <p>Overt monitoring of access to IT and other equipment</p> <p>Overt monitoring of access to IT and other equipment is allowed under the data protection regulations and is governed by the Information Technology Act, 2000 and the Code of Business Conduct.</p> <p>Covert monitoring of access to IT and other equipment</p> <p>See above.</p> <p>Reporting hotlines (anonymous)</p> <p>This measure is widely used in India. The establishment and use of a reporting hotline is generally set down in the Code of Business Conduct or Certified Standing Orders, and normally includes the process for investigating and responding to reports of suspicious activity. These documents may also specify the conditions of anonymity attaching to reporting hotlines.</p>
-------------------	---	--

		<p>Reporting hotlines (confidential)</p> <p>See above.</p> <p>Use of alerts/automated warning systems to identify unusual employee behaviour (out-of-hours activities, duplicate payments)</p> <p>See above.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>To prevent the unauthorised removal, transfer or theft of vital or sensitive company data or information the employer may safeguard its interests in the Code of Business Conduct by disallowing or allowing only limited use (as the case may be) of personal cellphones, laptops, pen drives, etc. This is legitimate and accepted practice in India.</p> <p>Monitoring of communication channels owned and operated by an employer (whether telephone lines, mail, email or internet) is accepted and usual practice amongst offshoring or outsourcing organisations. The basis on which such monitoring may be undertaken is set down in the Code of Business Conduct and may be specified in Certified Standing Orders.</p>
4.8	Formal investigations	<p>Is there a licensing regime covering investigators?</p> <p>The Private Security Agencies (Regulation) Act, 2005 provides for the regulation of private security agencies and for matters connected with or incidental to such regulation.</p> <p>The Private Detective Agencies (Regulation) Bill 2007 is intended to provide a strict framework for controlling detective agencies through a system of licensing and creates regulatory authorities at central and state levels. It will set penalties for offences at work including the violation of a person's right to privacy and freedom. Relevant sections include s. 2 sss (g), (h) and (i):</p> <p>(g) 'private detective work' means collection of information by a licensed private detective agency in a manner lawful for such an objective</p> <p>(h) 'private detective agency' means a person or a body of persons or a firm or a company holding a valid licence to carry out detective work for remuneration or reward on an agency basis for other persons and</p> <p>(i) 'private detective agent' means a person who carries out private detective work for a private detective agency.</p> <p>Currently this bill still seems to be in consultation stages with Government.</p>

Physical surveillance (overt or covert)

This is covered under the Code of Business Conduct. It is a legitimate right of the employer to protect its property whilst the employee or visitor is on its premises. Thus overt or covert CCTV surveillance in the workplace is accepted and practised with the proviso that there should be no surveillance in changing rooms, rest rooms and toilets.

The use of surveillance activities outside an employer's premises is not normal practice. However, in rare cases, where collecting evidence concerning the activities of an employee that is necessary to protect the interests of the organisation, a third-party, licensed security agency may be used to track the movements of that employee if this is in contemplation of action against that individual in a civil court or Labour Court.

Electronic surveillance (e.g. tracking devices)

See above.

Visual and communication surveillance (using cameras, video or CCTV)

See above.

Communication intercept (including oral, written and electronic communication including bugging devices)

Interception of personal telephone calls by the employee can be undertaken only by the police after obtaining specific permissions from the appropriate government authorities. However, the employer can undertake to do so at the workplace under the Information Technology Act, 2000 and the Code of Business Conduct if it applies to cellphones provided by the company for official use, or to on-premises landlines.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

This is covered under the Code of Business Conduct and is a legitimate right of the employer.

Formal interviews of staff

There is no restriction on an employer interviewing its own employees at the workplace and they are expected to cooperate in fact-finding procedures.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

Analysis of logs of phone, electronic mail and website activity is permitted only when related to official transactions, and only where the equipment is provided by and belongs to the employer.

		<p>Bank account details of an employee, even though pertaining to the account to which salary is paid, cannot be accessed by the employer or a private investigator appointed by the employer. This information can only be accessed by the police.</p> <p>Credit card details/information can be accessed by the employer if the card is in the employer’s name, the employer pays any subscription fee and the card is provided only for the official use of the employee.</p> <p>Search and seizure of evidence, whether electronic or physical (overt or covert)</p> <p>Search and seizure of evidence is allowed only on the premises of the employer and only if the property belongs to the employer and transactions are official and/or from official equipment. However, in the event criminal charges are contemplated against the employee, the employer or other employees cannot search or seize evidence as this may constitute tampering with evidence. In such a situation, the area concerned should be closed off until the police can attend.</p> <p>Is it either usual or necessary to involve the police in investigations?</p> <p>If the employee has violated the criminal laws of India, the employer may prefer to involve the police in investigations. Serious offences are normally referred to the police. The employer may hold a parallel internal investigation in order to instigate disciplinary action against the employee.</p> <p>If the police are involved, at what stage in the investigation does this generally occur?</p> <p>The police should be involved from the outset of the investigation.</p> <p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>The scene of any crime/offence must be cordoned off and no handling of or tampering with data, papers or evidence relevant to the investigation should be undertaken by the employer or other employees. The employer and other employees must cooperate with the police so that the investigation can be completed expeditiously.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>Every citizen is expected to inform the police about the commission or likely commission of a ‘cognizable’ offence.</p> <p>Section 39 of the Code of Criminal Procedure, 1973 specifies the offences to be reported and s. 202 of the Indian Penal Code contains the punitive provisions for the failure to report such offences.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

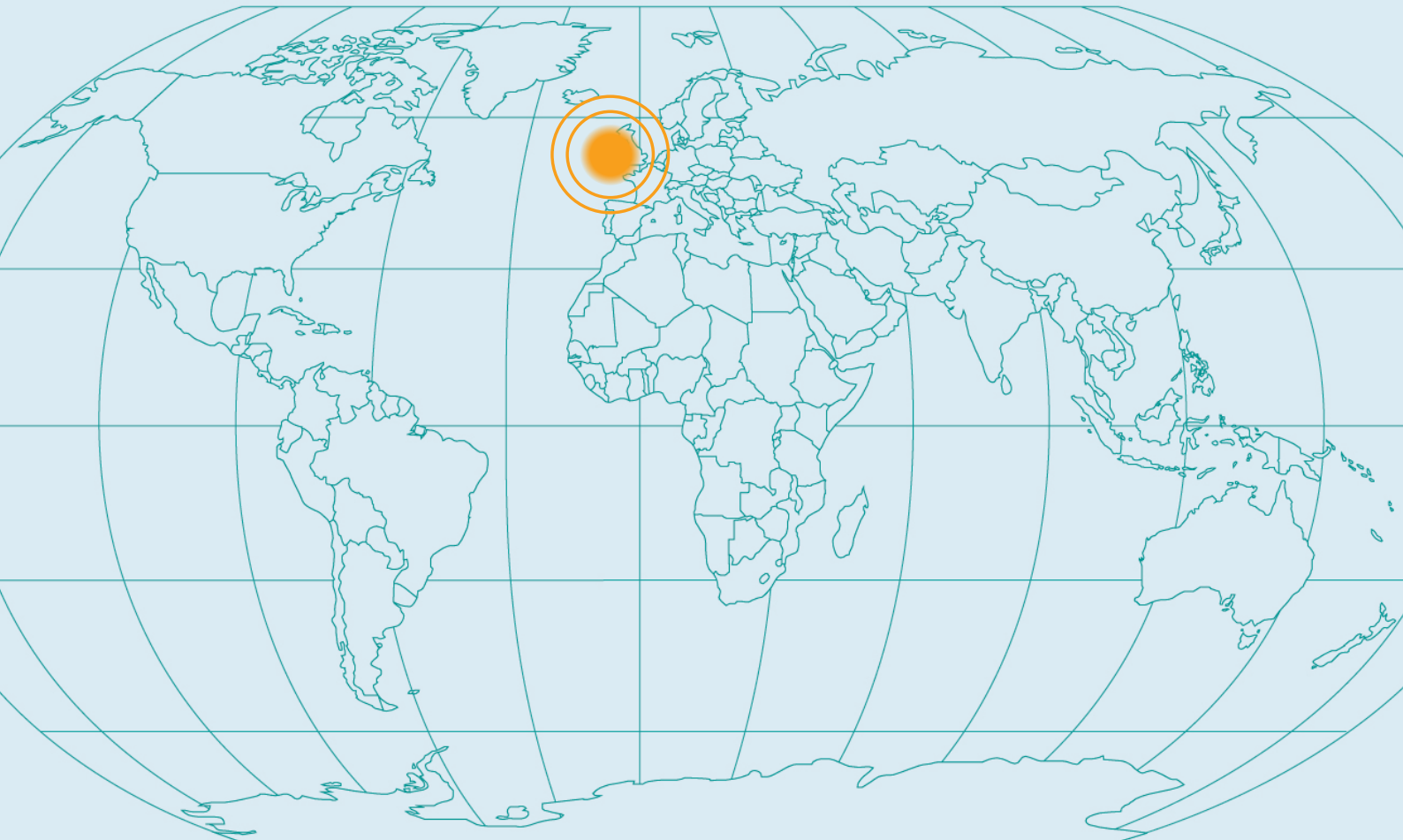
CPNI

Centre for the Protection
of National Infrastructure

SECURITY WATCHDOG
Part of Capita plc

Ireland (Republic of)

Personnel Security in Offshore Centres



Ireland (Republic of)

- 1** Introduction
- 2** Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3** Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4** Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1	Introduction	<p>Ireland has become a popular outsourcing destination for industries such as e-commerce, owing to its reputation for high-quality IT, financial and customer service skills together with an excellent infrastructure. Over recent years its competitiveness has declined in relation to other, lower-cost centres such as India and China. As a member of the European Union (EU), Ireland has implemented EU directives in relation to data protection and privacy. It has well-developed legislation relating to employment, including employee and employer rights, and processes for the resolution of labour disputes, either formally or informally.</p> <p>In Ireland, an employer’s rights to impose security procedures such as monitoring employee communications must be balanced against the rights of employees to privacy. An employer can be expected to take reasonable steps to detect and prevent criminal activities and measures imposed should be proportionate to the risks faced.</p> <p>In their conditions of employment employees should be made aware of their rights and responsibilities, and should be advised of measures that may be undertaken by the employer to protect its assets (e.g. use of surveillance cameras or monitoring of communications). It is good practice for an employer to advise its employees of its disciplinary and grievance policies and their rights of redress, including measures allowing employees to respond to breaches of company policy.</p>
2	Personnel security measures during recruitment	
2.1	Culture of screening	<p>Pre-employment screening is an established and accepted personnel security measure in Ireland. Whether pre-employment screening is conducted is dependent on the industry sector. It may include security matters (for example, whether the prospective employee has a criminal record) as well as qualitative matters (for example, the suitability of the individual to the post applied for).</p> <p>Under the Employment Permits Act 2003 (amended 2006), employers are required to verify a prospective employee’s right to work in Ireland.</p>
2.2	Major laws and regulations applying to pre-employment screening	<p>The major laws and regulations covering pre-employment screening in Ireland include the following:</p> <ul style="list-style-type: none"> • The Equality Act 2004 amended the Employment Equality Act 1998, the Pensions Act 1990 and the Equal Status Act 2000, to make further and better provision in relation to equality of treatment in the workplace and elsewhere; to implement the principle of equal treatment between persons irrespective of racial or ethnic origin; to establish a general framework for equal treatment in employment and occupation; and to implement the principle of equal treatment of men and women as regards access to employment, vocational training and promotion, and work conditions. • The Data Protection Act 1998 and the Data Protection (Amendment) Act 2003 bring Irish law into line with the EU Data Protection Directive 95/46/EC. Criminal penalties may be imposed for violations of the Act. The Act defines the role of a data controller and imposes on data controllers eight obligations, to:

1. obtain and process information fairly;
2. keep data for one or more specified, explicit and lawful purposes;
3. use and disclose data only in ways compatible with these purposes;
4. keep data safe and secure;
5. keep data accurate, complete and up to date;
6. ensure that data is adequate, relevant and not excessive;
7. retain data for no longer than necessary for the purpose or purposes; and
8. give a copy of his/her personal data to an individual, on request.

The Act provides additional protection for 'sensitive' data, which is defined as information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, the commission or alleged commission of an offence and any proceedings arising therefrom.

Enforcement of the data protection laws is overseen by the office of the Data Protection Commissioner who has powers to investigate complaints and prosecute offenders.

- The **ePrivacy Regulations 2011 (SI 336 of 2011)** deal with data protection for telephone, email, SMS and internet usage. They give effect to the EU ePrivacy Directive 2002/58/EC (as amended by Directives **2006/24/EC** and **2009/136/EC**).
- The **Employment Permits Act 2006** was introduced by the Department of Enterprise, Trade and Employment and came into effect from 1 February 2007. The Department considers that there should be a sufficient labour pool within the EEA (and Switzerland) and that employees outside this area should be permitted to work in Ireland only in exceptional cases. The Employment Permits Act introduced a number categories of permit that apply to non-EEA nationals:
 - work permits, issued to employees with salaries of €30,000 or more. These are granted for an initial period of two years, and are renewable for a further period of three years. The Department has imposed strict conditions on issuing work permits, including the requirement to advertise posts in local and national newspapers and non-issue of work permits for certain occupational sectors. Work permits are very rarely issued to those on salaries of less than €30,000.
 - green card permits were introduced by the 2006 Act. These are essentially employment permits for most positions with annual salaries of more than €60,000. For certain occupations, green cards may be issued where the annual salary is between €30,000 and €60,000. The green card is issued for an initial period of two years, may be renewed for an indefinite period and permanent residency may be sought.

		<p>– intra-company transfer permits were reintroduced under the new employment permits system. They are available to senior management, key personnel or those participating in a training programme, provided they earn an annual salary of at least €40,000 and have been working for the overseas employer for at least 12 months prior to the transfer. Intra-company transfer permits are normally granted for an initial period of 24 months, but may be renewed subject to a maximum stay of 5 years. Normally, a maximum of 5% of the workforce is permitted to hold intra-company transfer permits (except for certain defined situations such as small companies or start-ups where the limit may be extended to 50%).</p> <p>University graduates may apply to remain in Ireland for up to six months following receipt of their examination results, allowing them sufficient time to seek employment. If the individual subsequently finds a position, he or she may apply for a work permit or green card (subject to the absolute limit that not more than 50% of a workforce should constitute non-EEA nationals).</p>
3	Pre-employment checks	
3.1	Identity check	<p>Checks of name and address are widely undertaken.</p> <p>Identity is verified using the following documents:</p> <ul style="list-style-type: none"> • passport • driver’s licence • marriage certificate or • birth certificate.
3.2	Checks on eligibility to work	<p>Non-EEA nationals must show a valid employment permit; EEA nationals must show evidence of their nationality. If the employer is applying for an employment permit on his or her behalf, the candidate must show evidence of nationality (passport or birth certificate).</p> <p>Employees must provide employers with their permit documentation, as well as their Garda National Immigration Bureau (GNIB) card, which shows the right of the individual to reside in Ireland.</p> <p>An employer may verify work permit documentation with the Department of Enterprise, Trade and Employment. In most cases the work permit will be applied for by the employer, before the employee commences work.</p> <p>Note that, under the Employment Permits Act 2006, it is illegal for an employer to deduct the cost of a work permit/green card from an employee’s pay.</p> <p>Further information is available at www.entemp.ie.</p>
3.3	Residency checks	<p>Checks of current and former addresses are generally undertaken.</p> <p>Residency data may be verified against the voters’ roll, which is a public document. It is held in local post offices, police (An Garda Síochána) stations and public libraries. It can also be checked online at www.checktheregister.ie/PublicPages/Default.aspx?uiLang</p>

3.4**Criminal record checks****Name of certificate**

Police Certificate or Data Access Request.

Department that holds records

Garda Central Vetting Unit.

Where to apply within country

Garda Central Vetting Unit,
Garda Criminal Records Office,
Data Protection Processing Unit,
Racecourse Road,
Thurles,
Co. Tipperary,
Republic of Ireland.

Website: <http://www.garda.ie/Controller.aspx?Page=66>

Local Garda Stations – a link to their contact details can be found at: <http://www.garda.ie/Stations/Default.aspx>.

How to apply within country**Police Certificate**

Individuals may also apply to their local district superintendent for a Police Certificate. Officially, a Police Certificate will not be issued for pre-employment screening processes. However, it is understood that certificates may have been obtained for this purpose.

The application is a free-form letter that must include:

- the individual's full name (including maiden name where appropriate)
- date and place of birth (or a copy of the birth certificate)
- current address
- all addresses lived at in Ireland and the dates for each
- the place and purpose for requesting a Certificate
- a copy of a passport, driving licence or similar type of identification and
- a stamped, self-addressed envelope.

Subject Data Access Request

Applications must be made in writing, either in free form or using the application form. Details of the process and who to contact can be found on the Garda website at <http://www.garda.ie/Controller.aspx?Page=8382&Lang=1>

The form should be printed and completed, providing the following information:

- the type of information request (i.e. a request for all criminal record data under the Data Protection Act 1988/2003)
- full name of applicant, including any previous names where applicable
- date of birth
- address(es)
- date of application
- return address for information and
- the applicant's signature.

		<p>The completed application form should be posted to the Garda Central Vetting Unit along with payment of the required fee and a copy of the candidate's:</p> <ul style="list-style-type: none"> • passport • birth certificate and • driving licence or other form of identification. <p>Who can apply</p> <p>Access to criminal record data for UK employment purposes is restricted. The Garda advises that under data protection legislation the only form of disclosure available to British employers is a Data Access Request. However, the same legislation prohibits employers from requesting this from prospective employees. The Garda Central Vetting Unit provides vetting disclosure for certain types of employment.</p> <p>Individuals may also apply to their local district superintendent for a Police Certificate. Officially, a Police Certificate will not be issued for pre-employment screening processes. However, it is understood that certificates may have been obtained for this purpose.</p> <p>Any individual may obtain access to his or her own criminal record under the provisions of the Data Protection Act 1988/2003. Irish legislation allows an individual to provide consent for disclosure to be made to a third party.</p> <p>Cost, payment and turnaround</p> <p>Police Certificate</p> <p>The certificate is issued free of charge, within three weeks.</p> <p>Data Access Request</p> <p>There is a processing fee of €6.35 for a Data Access Request. A personal cheque, money order or postal order made payable to 'The Accountant, Department of Justice' should be attached to the application form.</p> <p>The results of a Data Access Request will be issued within 40 days.</p> <p>Legislation</p> <p>The Data Protection Act 1988 and the Data Protection Amendment Act 2003.</p> <p>Further information can be obtained from the CPNI guidance on <i>Overseas Criminal Record Checks</i> which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/</p>
3.5	Education checks	<p>Education checks are commonly carried out in Ireland. Such checks typically seek to confirm the educational establishment attended and the dates of attendance.</p> <p>Education checks are normally undertaken directly in writing with the establishment(s) concerned. Generally the consent of the individual is required by establishments before divulging information. Information is provided in accordance with the Data Protection Act 1998 (amended 2003).</p>

3.6	Qualification checks	<p>Qualification checks are commonly undertaken in Ireland and normally seek to confirm:</p> <ul style="list-style-type: none"> • subjects studied • grades/diplomas or degrees obtained • professional qualifications attained, and • status of (professional) membership. <p>Qualification checks are normally undertaken directly in writing with the establishment(s) concerned. Usually this is by mail/email or fax, although some organisations (for example professional bodies) may issue information on membership online. Generally the consent of the individual is required before information will be released.</p> <p>Any information must be provided in accordance with the Data Protection Act 1998 (amended 2003).</p>
3.7	Employment references	<p>Employment references are commonly taken up in Ireland, directly with former employers of the candidate, with the agreement of the prospective employee. Employers might not provide character references (see below).</p> <p>Under the Employment Equality (Amendment) Act 1998/2004 and the Data Protection (Amendment) Act 1988/2003, the prospective employee must consent and give permission to the prospective employer to obtain this information. Therefore it is common practice to request explicit consent of the prospective employee to obtaining this information.</p> <p>Character references from previous employers</p> <p>Character references are commonly taken up, directly with referees provided by the employee. There are no specific legal considerations.</p> <p>Character references from persons of standing in the community</p> <p>In Ireland character references may be taken from persons of standing in the community (e.g. professionals, members of the judiciary, police services, etc). There are no specific legal considerations.</p>
3.8	Financial/ credit checks	<p>Technically, the Data Protection (Amendment) Act 1998 (amended 2003) prohibits the obtaining of financial information for confidentiality reasons. However, in practice this information may be supplied by a prospective employee depending on the requirements/ needs of the position applied for as part of the conditions of employment as agreed between the employee and employer.</p> <p>Where credit checks are carried out as part of the pre-employment security screening process they will include details of judgments, bankruptcies, director disqualifications and checks on the electoral roll. Credit checks may be undertaken through a commercial credit-referencing bureau, such as Experian or Equifax.</p>

3.9	Substance abuse screening	<p>Substance abuse screening may be used on limited occasions if an employer has grounds for believing that an employee is misusing substances. It would be normal practice to ask the human resources department of the organisation to take further steps.</p> <p>In the context of pre-employment screening, data of this nature are covered by the Data Protection (Amendment) Act 1988/2003 and therefore are not accessible by prospective employers.</p>
3.10	Occupational health checks	<p>This type of information is not available under the Data Protection (Amendment) Act and the Irish Constitution (unless volunteered by the individual). An individual would need to provide explicit consent to such checks.</p> <p>The results of occupational health checks are also covered by the Data Protection (Amendment) Act 1988/2003 and an individual may challenge a data controller if he or she considers that the information held is inaccurate.</p>
4 Personnel security measures during employment		
4.1	Legal requirements	<p>The following laws and regulations are relevant to personnel security measures during employment:</p> <ul style="list-style-type: none"> • the Equality Act 2004, as detailed above • the Data Protection Act 1988 (amended 2003): more information is available from the Data Protection Commissioner (see www.dataprotection.ie) • the Employment Permits Act 2006 (see Section 2.2) • the Constitution of Ireland, Articles 40–44 incorporate the fundamental right of equality before the law. The state is bound to protect ‘the personal rights of the citizen’ and in particular to defend ‘the life, person, good name and property rights of every citizen’ (Article 40.2). Individuals have the right under the Irish Constitution to join a trade union. The single umbrella organisation in Ireland for trade unions is the Irish Congress of Trade Unions. It represents the interests of employees both in the Republic of Ireland and in Northern Ireland. In certain organisations the employee must join a particular trade union. Whether this is legal under the Constitution has not yet been tested in a court of law. However an employer cannot require an employee to join a trade union after he or she has accepted a job offer. Dismissal for trade union activity or membership is automatically unfair under the Unfair Dismissals Act 1977 to 2007 (see below). There is no requirement for any particular length of service before bringing an action for unfair dismissal in such a case. Alternatively, a case may be brought to a Rights Commissioner or to the Employment Appeals Tribunal (see below). • the Unfair Dismissals Acts 1977 to 2007 protect employees from being unfairly dismissed by applying criteria by which dismissals are to be judged unfair, and by providing an adjudication system and redress for an employee whose dismissal has been found to be unfair

		<ul style="list-style-type: none"> • the Minimum Notice and Terms of Employment Act 1973 lays down the minimum periods of notice to be given by employers and workers when terminating a contract; it applies in most employments where employees have 13 weeks of continuous service • the Industrial Relations (Amendment) Act 2012 has some provisions for terms of employment although it largely focuses on pay rates for employees • the Copyright and Related Rights Act 2000 permits unannounced searches and imposes strong penalties for theft or misuse of software; this is particularly relevant in Ireland, which has a well-developed e-commerce sector • the Interception of Postal Packets and Telecommunication Messages (Regulation) Act 1993 prohibits the use of wiretapping and electronic surveillance measures • the Criminal Justice (Theft and Fraud Offences Act) 2001 covers offences such as burglary and robbery as well as misuse of computer equipment and • the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 includes provisions for tackling money laundering. The Act implemented the provisions of the Third EU Money-Laundering Directive. Organisations in the financial services sector and certain designated professions (such as accountants, solicitors, high-value goods dealers, money service bureaux) must take steps to identify their customers and report suspicions of money laundering to the police. <p>The Labour Relations Commission promotes the development and improvement of Irish industrial relations policies, procedures and practices through the provision of appropriate time and effective services to employers, trade unions and employees.</p> <p>The Commission provides:</p> <ul style="list-style-type: none"> • an industrial relations conciliation service • an industrial relations advisory and research service • a Rights Commissioner service • a Workplace Mediation service and • assistance to Joint Labour Committees and Joint Industrial Councils in the exercise of their functions. <p>The Labour Relations Commission was established on 21 January 1991 under s. 24 of the Industrial Relations Act 1990.</p> <p>The Employment Appeals Tribunal is an independent body established to provide a fast, inexpensive and less formal means for adjudicating disputes on employment rights.</p>
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	<p>The employer’s rights are protected by legislation as set out above, including the Data Protection Act 1988 (amended 2003) and by copyright and intellectual property law. In addition, the contract of employment will set out duties and obligations of the employee towards the employer.</p>

4.4	Local legislation that specifically governs the rights of the employee	<p>The National Employment Rights Authority provides guidance on the rights of both employers and employees. It is responsible for monitoring employment conditions through its inspection services and can enforce compliance and seek redress. It covers a range of employment rights including:</p> <ul style="list-style-type: none"> • wages • annual leave • working hours • redundancy • dismissal and • notice. <p>As set out above, the rights of the employee are covered by the Irish Constitution as well as under specific employment and labour law.</p>
4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	<p>An employee may bring action under legislation as set out above (for example, misuse of personal data under the Data Protection Act; the Unfair Dismissals Act and the Minimum Notice and Terms of Employment Act). In addition, he or she may seek redress through their trade union or through a Rights Commissioner or the Employment Appeals Tribunal (for the latter options, an employee must file a written notice of claim within six months of the date of dismissal).</p> <p>An employee may also seek redress under common law, but they must choose to seek redress either under common law or under the Unfair Dismissal Acts 1977 to 2007.</p> <p>Most employers in Ireland also set out grievance/disciplinary procedures as part of their conditions of employment.</p>
4.6	What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?	<p>Employers in Ireland must comply with the conditions of the Unfair Dismissals Acts 1977 to 2007 and must ensure that actions comply with Irish legislation, which affords protection to employees in certain circumstances.</p>
4.7	Availability of security measures	<p>Restriction of access to the premises</p> <p>Employers are permitted to control access to the premises. However, should this give rise to the capture of personal details (e.g. use of biometric information such as fingerprint scanners to control entry) the principles of the Data Protection Act 1988/2003 (including proportionality, fair obtaining, accuracy and security of personal data) must be observed at all times.</p>

Restriction of access to certain rooms/zones on the premises

See above.

Physical screening (on entry/exit)

See above.

Prohibition of removal of data from the premises (hard-copy)

Removal of data is covered in particular by the conditions of the Data Protection Act 1988/2003 and by the Criminal Justice (Theft and Fraud Offences Act) 2001.

Prohibition of removal of data from the premises (electronic)

See above.

Visual surveillance (CCTV or other cameras), either overt or covert

Overt use of CCTV and other monitoring is generally permissible, although it might not be acceptable in 'private' areas such as toilets or changing rooms where its use is likely to be considered disproportionate, excessive or an invasion of personal privacy. Storage and use of CCTV data is also subject to provisions in the Data Protection Act 1988/2003.

Covert use of surveillance cameras or CCTV is not generally lawful. It may be permissible only in situations where the data is gathered for the purpose of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies an actual involvement of the police (An Garda Síochána) or an intention to involve the police.

Overt monitoring of access to IT and other equipment

Overt monitoring is used in Ireland. Under the provisions of the Data Protection Act 1988/2003, the employer has the right (and duty) to ensure and maintain security of data. In Ireland it is good practice for an employer to detail its policy regarding monitoring of access to IT and other equipment.

Covert monitoring of access to IT and other equipment

In Ireland it is good practice for an employer to detail its policy regarding monitoring of access to IT and other equipment. Covert monitoring should only be used in situations where the risk presented is proportionate to the action by the employer (e.g. an employee is suspected of committing a crime).

Reporting hotlines (anonymous)

Whistleblowing hotlines are commonly used in Ireland to allow employees to report suspected breaches of law or regulation, or other questionable actions (e.g. accounting manipulation).

Reporting hotlines (confidential)

See above.

		<p>Use of alerts/automated warning systems to identify unusual employee behaviour (out of hours activities, duplicate payments)</p> <p>Such measures may be used provided they do not contravene employment or data protection legislation. Employers should consider the proportionality of responses to specific risks and ensure that actions do not unnecessarily impact on the employee’s right to personal privacy.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>As a matter of good practice, any policy regarding monitoring of communications by the employer should be clearly set out in the employment contract. The procedures used to monitor employees should be proportionate to the risks faced. Employers should avoid monitoring communications (private or otherwise) covertly, except in situations where there is concern that a crime has been committed (under which circumstances the employer has a potential duty under law to investigate). There has been increasing concern in Ireland for some years about monitoring of employee activity (e.g. internet usage) although this has not yet led to specific restrictions apart from what is contained in existing data protection law.</p>
4.8	<p>Formal investigations</p>	<p>Is there a licensing regime covering investigators?</p> <p>Investigators in Ireland are licensed by the Private Security Authority which issues Private Security Service Contractors’ licences (companies, partnerships and sole traders providing security services) and Private Security Service Employee licences.</p> <p>In addition, the Employment Regulation Order (Security Industry) 2005 provides for:</p> <p>‘Security operatives, namely persons employed to provide a security service for their employer. “Security Service” means a service of a security or surveillance nature, the purpose of which is to protect persons and property.’</p> <p>The primary functions of a security operative are:</p> <ul style="list-style-type: none"> • to prevent or detect theft, loss, embezzlement, misappropriation or concealment of merchandise, money, bonds, stocks, notes or other valuables • to prevent or detect intrusion, unauthorised entry or activity, vandalism or trespass on private property either by physical, electronic or mechanical means and • to enforce rules, regulations and policies related to crime reduction. <p>This regulation covers private investigation companies, static security duties and general security contracts.</p>

Physical surveillance (overt or covert)

Use of physical surveillance measures must comply with employment and data protection law. Given that such a measure is likely to be invasive, in practice its use would be restricted.

Electronic surveillance (e.g. tracking devices)

Use of electronic surveillance measures must comply with employment and data protection law. Given that such a measure is likely to be invasive, in practice its use would be restricted.

Visual and communication surveillance (using cameras, video or CCTV)

An employer's use of visual and communication surveillance should ideally be clearly set out in the employer's policies, as part of the employment contract. Use of such measures should be proportionate to the threat. It is unlikely that covert surveillance would be acceptable under data protection legislation except in situations where a crime is suspected. In addition, employers should not retain data longer than necessary.

Communication intercept (including oral, written and electronic communication including bugging devices)

Communication interception is not legal in Ireland under the provisions of the Interception of Postal Packets and Telecommunication Messages (Regulation) Act 1993.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

The right to use such measures by an employer is generally stipulated in the conditions of employment. As above, measures used should be proportionate.

Formal interviews of staff

Formal interviews of staff may be undertaken provided they are carried out in accordance with employment legislation and common law.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

This type of measure may be used in Ireland provided it does not invade personal privacy and is proportionate to the threat. Employers do not have a right to monitor personal activities (for example, use of personal telephones). It is good practice for employers to set out their email, telephone and internet usage policies clearly in their terms of employment.

		<p>Search and seizure of evidence, whether electronic or physical (overt or covert)</p> <p>Search and seizure of evidence is not permitted unless obtained by execution of a search warrant obtained from the courts. In Ireland search warrants can only be executed by the police.</p> <p>If an organisation or business has good reason to believe that a criminal offence has been committed, it should take appropriate steps to ensure the safe custody of evidence and to prevent wrongdoing. It is common practice for organisations to undertake internal enquiries (with or without the assistance of private, third-party investigators) to determine whether a criminal offence might have been committed. If the organisation considers that a criminal offence has taken place, it should involve the police who will obtain search warrants and conduct lawful searches to ensure that evidence is collected in a legal manner.</p> <p>Is it either usual or necessary to involve the police in investigations?</p> <p>In Ireland the police are mandated to conduct all criminal investigations on receipt of complaints. Organisations that suspect they are the subject of a crime should report the matter to the police.</p> <p>If the police are involved, at what stage in the investigation does this generally occur?</p> <p>The police should be involved at the point a crime is discovered and is reported to them.</p> <p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>In practice, the police must be involved in criminal cases, to secure the evidential integrity of the crime scene.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>The Criminal Justice Act 1994 obliges an employer to report suspicions of money laundering to the police.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

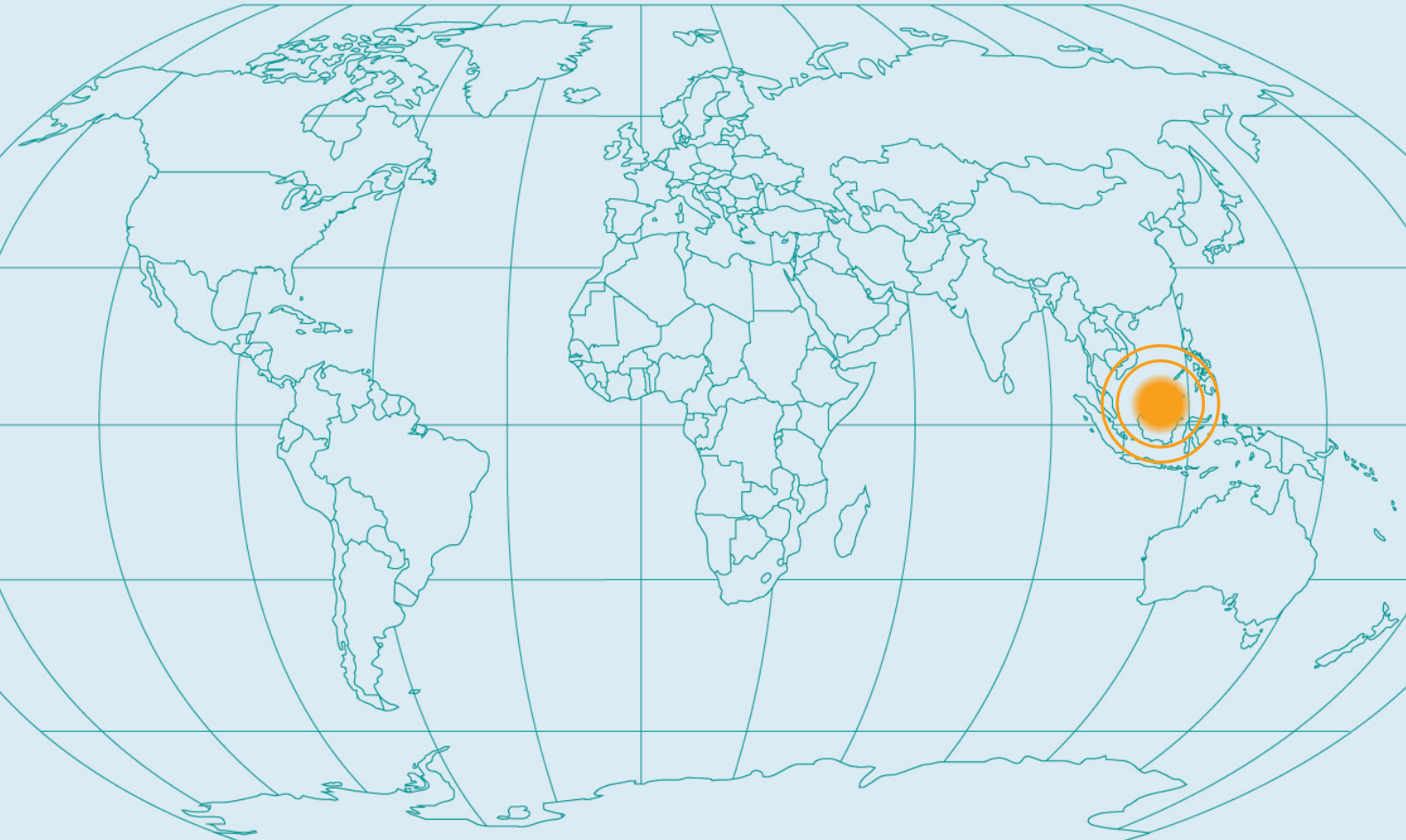
CPNI

Centre for the Protection
of National Infrastructure

SECURITY WATCHDOG
Part of Capita plc

Malaysia

Personnel Security in Offshore Centres



● Malaysia

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1	Introduction	<p>The outsourcing industry in Malaysia has grown by 15% since 2009 to reach a market size of USD1.7bn in 2012. Although the sector only employs about 48,000 people, the development of the industry means that this workforce is projected to increase substantially over the next five years.</p> <p>Malaysia has a strategic advantage in that it is central in a region that represents a market of over half a billion consumers, averaging a combined gross domestic product of USD737 billion.</p> <p>A business-focused government propels the country to provide for a smooth and conducive business environment, backed by appropriate focus on information security, minimal customs controls, beneficial tax incentives, relaxed monetary exchange controls and attractive incentives for R&D. This type of environment is attractive to investing businesses and offers competitive advantages over other offshoring destinations.</p> <p>Malaysia’s well-educated, multi-ethnic workforce continues to grow as a knowledge- and service-based economy. This is coupled with a workforce that holds a strong work ethic.</p> <p>Malaysia produces an annual output of over 135,000 graduates with Bachelor’s degrees; many with experience in customer relations, finance and accounting, IT and Human Resources (HR) services. The workforce is readily available and highly skilled, proving to be cost-efficient with high levels of productivity that attract prospective international employers.</p> <p>Malaysia’s cities are well connected via land and air transportation services, in addition to high-speed broadband access and globally competitive telecom services, which are further enhanced by the latest fibre optics cabling.</p>
2	Personnel security measures during recruitment	
2.1	Culture of screening	<p>As a growing industrial society pre-employment screening has still to be commonly applied within Malaya. In the private sector the level of pre-employment screening undertaken is generally commensurate with the roles and responsibilities of the individuals concerned. For example, the employer may screen prospective candidates for middle or senior management roles, or those who have access to financially sensitive information or assets under control of the organisation. This practice is usually reserved to the larger corporate employers and multinationals that are influenced by international policies.</p> <p>Pre- employment screening for junior employees, where used, is generally limited to verification of previous employment only.</p>

<p>2.2</p>	<p>Major laws and regulations applying to pre-employment screening</p>	<p>There are a number of labour laws in Malaysia that have a variety of different influences on employment in Malaysia.</p> <p>The Employment Act 1955 (amended 2012) lays down minimum terms and conditions (mostly of monetary value) for certain categories of employee:</p> <ul style="list-style-type: none"> • any employee whose monthly wages are less than MYR2,000 • any person employed in manual work including artisans, apprentices, transport operators, supervisors or overseers of manual workers, persons employed on vessels and domestic servants even if their wages exceed MYR2,000 per month • any ‘foreign domestic servant’ who is not a citizen or permanent resident and • part-time employees. <p>The Industrial Relations Act 1967 provides ways for settlement of trade disputes between employers and workmen. This term means any person, including an apprentice, employed by an employer under a contract of employment to work for hire or reward and for the purposes of any proceedings in relation to a trade dispute includes any such person who has been dismissed, discharged or retrenched in connection with or as a consequence of that dispute or whose dismissal, discharge or retrenchment has led to that dispute. (Not limited by size of wages.)</p> <p>Beside the difference in definition, the two Acts also provide different benefits to workers. The Employment Act is more focused on monetary benefits (annual leave with pay, sick leave with pay, maternity allowance, overtime and so on). Failure to provide any of those benefits is an offence for which an employer can be prosecuted. The Industrial Relations Act is more of a persuasive nature in that industrial problems are solved as far as possible through negotiation and conciliation.</p> <p>The Trade Unions Act 1959 regulates trade union registration and the uses of trade union funds.</p> <p>Malaysia’s Personal Data Protection Act 2010 (PDPA) took effect as of 15 November 2013, introducing a new privacy regime for the first time. A series of regulations have been issued to implement the Act’s provisions. Data controllers had three months from the date of enactment to comply with the PDPA to avoid enforcement.</p> <p>The Personal Data Protection (Class of Data Users) Order 2013 requires certain organisations to register under the PDPA as data users with Malaysia’s new Personal Data Protection Commissioner. These include:</p> <ul style="list-style-type: none"> • banking and financial institutions • communications service providers • tourism and hospitality providers • insurers
-------------------	---	---

		<ul style="list-style-type: none"> • real estate firms • education bodies • direct marketing organisations • transportation firms and • utility providers. <p>The Personal Data Protection (Registration of Data Users) Regulations 2013 set out the costs of registration, which apply for a period of 24 months prior to renewal. Failure to register as a data user could result in a fine of up to MYR500,000 and imprisonment for up to three years.</p>
3	Pre-employment checks	
3.1	Identity check	<p>Every Malaysian citizen and Malaysian Permanent Resident is issued with a national identification card. The compulsory identity card for all Malaysian citizens aged 12 years or above (MyKad) was one of the first fully biometric cards ever issued. It has multiple functions including a driving licence and ATM card amongst others. Its core function is proof of citizenship. Card holders are required to keep their card up to date under law.</p> <p>Permanent Residents of Malaysia are issued with a MyPR.</p> <p>For foreigners working in Malaysia, the common means of identification is the passport.</p> <p>Other identity checks would include producing a copy of the previous income tax statement or Employees' Provident Fund statement.</p> <p>Prospective employers can request a candidate to produce the latest EPF statement as part of their recruitment verification records. The individual may refuse to provide this information and there is no legal obligation on them to produce the statement.</p>
3.2	Checks on eligibility to work	<p>In Malaysia employers seeking to employ foreign nationals must apply for a work permit to the Immigration Department of Malaysia (Jabatan Immigresen Malaysia) before the foreigner can commence work.</p> <p>An employer may not access previous work permit or employment applications relating to a prospective employee, nor find out whether such permits have been previously revoked. A new work permit is required for each separate employment although extensions can be granted.</p>
3.3	Residency checks	<p>The prospective employee's residency is stated on their MyKad (or MyPR) and, where applicable, their application for an employment permit. A number of commercial data aggregators provide verification services (for identity and residency) that are based on data sourced from business interest records, and/or litigation and bankruptcy records.</p> <p>Apart from the information listed on the MyKad and employment documents, it is not possible for an employer to access residency data. For example, electoral roll data in Malaysia is not a matter of public record.</p>

		<p>More traditional methods may then be required in such as requesting:</p> <ul style="list-style-type: none"> • lease and licence agreements • recent bank statements • a company letter stating the address (if a company is providing accommodation) and • a gas or electricity bill.
<p>3.4</p>	<p>Criminal record checks</p>	<p>Name of certificate</p> <p>Certificate of Good Conduct (CGC) (Sijil Kelakuan Baik).</p> <p>Department that holds records</p> <p>Central Criminal Registry (CCR), Royal Malaysian Police, Bukit Aman 50 560, Kuala Lumpur, Malaysia.</p> <p>Telephone: +60 (0) 3 2266 2222 Fax : +60 (0) 3 2070 7500 Email: rmp@rmp.gov.my</p> <p>Where to apply within country</p> <p>Consular Division, Ministry of Foreign Affairs, Wisma Putra, 1, Jalan Wisma Putra, Precinct 2, 62602 Putrajaya, Malaysia.</p> <p>Telephone: +60 (0) 3 8887 4000/+60 (0) 3 8000 8000 Fax:+60 (0) 3 8889 1717 Email: skb_admin@kln.gov.my Website: www.kln.gov.my/web/guest/home/</p> <p>Sarawak Regional Office, Ministry of Foreign Affairs Malaysia, Level 14, Bangunan Sultan Iskandar, Jalan Simpang Tiga, 93300, Kuching, Malayasia.</p> <p>Telephone: +60 (0) 82 236146 Fax: +60 (0) 82 236983 Email: pwsarawak@kln.gov.my</p>

Sabah Regional Office,
Ministry of Foreign Affairs,
Block A, 7th Floor,
Kompleks Pentadbiran Kerajaan Persekutuan Sabah,
Jalan UMS,
88400,
Kota Kinabalu,
Malaysia.

Telephone: +60 (0) 88 220018

Fax: +60 (0) 88 488518

Email: pwsabah@kln.gov.my

How to apply within country

Online through the website at www.kln.gov.my (click on 'Certificate of Good Conduct' under the 'e-Consular' heading on the right-hand side of the page).

The documents required are:

- identity card
- passport details
- last employer in Malaysia
- details of higher education in Malaysia (if applicable)
- an uploaded passport-sized photo and
- non-Malaysians must upload a scan of their passport.

The application must then be submitted and the 'Application Acknowledgement' printed (this must be presented when collecting the CGC).

The application status will change to 'CERTIFICATE IS READY FOR COLLECTION' when the CGC is ready. The individual can obtain the CGC from the addresses above in the following ways:

In person

Take Application Acknowledgement Slip; a third party must carry a letter of authorisation to collect on behalf of the individual.

By post

Send the Application Acknowledgement Slip and an A4-sized, stamped-addressed envelope.

Who can apply

Individuals only; although third parties can collect the CGC (see above).

Cost

- In person – cash payment of MYR 20 or
- by post – bank draft/money order for MYR20 payable to 'AKAUNTAN NEGARA MALAYSIA'.

		<p>Turnaround</p> <p>One to two months.</p> <p>Legislation</p> <p>Registration of Criminals and Undesirable Persons Act 1969.</p> <p>Further information can be obtained from the CPNI guidance on <i>Overseas Criminal Record Checks</i> which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>
3.5	Education checks	<p>Education checks are often required by employees to establish that a prospective employee attended the educational establishments claimed.</p> <p>Typical information provided is dates of joining and leaving the educational institution; subject of study; courses (college, university); degree and final mark.</p> <p>This information would have to be specifically requested as it would not be volunteered.</p> <p>Application for such information must be made in writing and provide all known information, e.g. full name, date of birth, subject of study. Many universities and colleges have a standard process for dealing with such enquiries. The consent of the individual is required.</p> <p>Employers usually require candidates to provide original testimonials, degrees/diplomas and results slips for verification. Depending on the policies of the employer, further verification with the educational institution may be made, but this would require the consent of the individual.</p>
3.6	Qualification checks	<p>Verification of professional qualifications (academic or professional) is a regular part of pre-employment screening if undertaken.</p> <p>Typical information confirmed is dates of joining and leaving the educational institution or professional body; membership status (professional body) and status and type of qualification.</p> <p>In many cases, all known information must be provided. The institution will confirm information; however it will not volunteer any data. Often questions regarding the character of an individual will not be answered by educational institutions in writing, although a verbal character reference might be obtained from a tutor or professor who knows the individual.</p> <p>Fake documentation is widespread across the region so documentation alone should not be relied upon. Attendance at an educational establishment does not prove the individual graduated from that establishment. It is also important to verify that an individual is an active member of a professional body and has not left, been ejected from membership or failed to renew their membership.</p>

<p>3.7</p>	<p>Employment references</p>	<p>It is normal for employers to provide references in Malaysia. These may confirm basic information such as dates of employment, positions held and reason for leaving. They do not necessarily include character references although employers in Malaysia generally provide neutral or positive feedback regarding the prospective employee’s work attitude at the request of the employee, as is customary across the region.</p> <p>When requesting references in Malaysia, employers should refrain from asking questions relating to race, as Malaysia is a multiracial society, or questions about family situations and the impact on the candidate’s ability to work. Most employers will not provide information on salaries, sickness record, performance records or parental leave. Requests for references are made directly to the previous/current employers. The consent of the individual is required.</p> <p>Character references are not always given by previous employers. Previous employers may offer only verification of basic details of employment history and reason(s) for leaving. Character references from persons of standing in the Malaysian community may be requested and there is no legal restriction. Care should be exercised to ensure that the referees are independent of the candidate (i.e. are not related).</p>
<p>3.8</p>	<p>Financial/ credit checks</p>	<p>Malaysia is becoming more influential in the Islamic banking world and financial checks are becoming more common for employment purposes. These checks are typically reserved for persons applying for more senior roles and, in particular, those involving access to financial systems or controls. They may be undertaken at the pre-employment stage, on an ongoing basis or where suspicions or concerns arise as part of initial investigations.</p> <p>Since 2002 all individuals have been able to obtain their own credit report from their local branch of Bank Negara Malaysia free of charge.</p> <p>There are also numerous credit reporting agencies (CRAs) operating in Malaysia that employers can use. All CRAs in Malaysia operate under the Credit Reporting Agencies Act 2010. Typical sources of information would be:</p> <ul style="list-style-type: none"> • publication of legal proceedings in newspapers and government gazettes • Companies Commission Of Malaysia • Malaysia Insolvency Department or • CRA subscribers’ contribution. <p>Information may also include payment histories from public utility companies, landlords, government and statutory bodies and local councils.</p> <p>Costs depend on the provider and the subscription type. Requests for credit information will leave a record on the individual’s credit file.</p>

3.9	Substance abuse screening	<p>Malaysia has suffered from a significant drug abuse problem for many years. The government set a commitment to be drug-free by 2015. Although not legally mandatory under the Occupational Safety and Health Act 1994 the government have issued comprehensive guidelines on the application of drug testing for employers to support the initiative. These guidelines can be found here:</p> <p>http://library.unisel.edu.my/equip-unisel/custom/guidelines/file38.pdf.</p>
3.10	Occupational health checks	<p>Malaysia is taking great steps to be an industrialised nation by 2020. This entails heavy and extensive use of chemicals. This type of check aims for early identification of conditions, if any, that could present an increased risk of adverse health effects related to the task being performed.</p> <p>Based on the type of work being performed, duration of the task, materials in use and potential exposure, medical surveillance is either recommended or required for the job role.</p> <p>Components of medical surveillance include:</p> <ul style="list-style-type: none"> • pre-employment medical examination • record keeping and monitoring • return to work examinations • disability assessments • biological monitoring and • health monitoring.
4 Personnel security measures during employment		
4.1	Legal requirements	<p>The PDPA has introduced new rules regarding data privacy that should be applied when dealing with an employee’s personal information. Employers must ensure that they are appropriately registered if they are to continue to process employee data.</p> <p>All employers must adhere to the conditions of the Employment Act 1955 and the Industrial Relations Act 1967 throughout the period of employment.</p> <p>The Constitution of the Federation of Malaya is largely based on the British system. It outlines rules on the fundamental liberties of citizens, citizenship and the constitution.</p> <p>Computer crime in Malaysia is governed by the Computer Crimes Act 1997, which supports investigations into computer misuse for the purposes of crime. As the Act supports investigation by police officers, officers should be involved in the early stages of an internal investigation.</p> <p>Employer monitoring of employee phone calls, emails, and internet usage is permissible under Malaysian law. Under Malaysian property law, workplace email, telephone and computer contents are the property of the employer. However, care must be exercised in the use of such measure since the introduction of the data protection legislation in 2013.</p>

		<p>In Malaysia, the privacy of bank customers is protected under the Central Bank of Malaysia Act 2009 and the Financial Services Act 2013. These acts prohibit disclosure of information without the explicit consent of the customer. There are certain exceptions to these acts, for example requirements to report suspicions of money laundering activities. The Anti-Money Laundering and Anti-Terrorism Financing Act 2001 is the primary legislation to combat money laundering in Malaysia and is especially applicable to the financial services industry.</p>
4.2	Laws governing the rights of the employee or employer	<p>Both the Employment Act and the Industrial Relations Act detail the rights and duties of both employers and employees and the conditions of treatment that need to be met.</p> <p>If an employee breaches his or her employment contract, or is found guilty of misconduct or poor performance, the employer reserves the right to take disciplinary action to the point of dismissal.</p> <p>The Employment Act covers the basic terms and working conditions of certain groups of employees. No specific provision impacts on personnel security except that the employer has to ensure a safe and healthy workplace for its employees. Were employees in Malaysia to challenge an employer's use of the security procedures described in this report, recourse might be available through civil courts.</p> <p>Only employees who are covered under the Employment Act have recourse to unfair dismissal provisions under the Industrial Relations Act. The recourse available to employees who are not covered under the Employment Act is through civil litigation or via the relevant trade union if available.</p>
4.3	Local legislation that specifically governs the rights of the employer	See Section 4.2 above.
4.4	Local legislation that specifically governs the rights of the employee	See Section 4.2 above.
4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	If any procedures (see Section 4.2 above) are upheld, the employee appeal to the Director General, who would refer the matter to the Minister of Human Resources who in turn might refer the case to a court.

<p>4.6</p>	<p>What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?</p>	<p>A workman can appeal under s. 20 of the Industrial Relations Act 1967 which states:</p> <p>'Where a workman, irrespective of whether he is a member of a trade union of workmen or otherwise, considers that he has been dismissed without just cause or excuse by his employer, he may make representations in writing to the Director General to be reinstated in his former employment; the representations may be filed at the office of the Director General nearest to the place of employment from which the workman was dismissed.'</p> <p>All appeals must be lodged within 60 days from the date of the dismissal. If justified the Director General would refer the matter to the Minister of Human Resources who in turn might refer the case to a court.</p>
<p>4.7</p>	<p>Availability of security measures</p>	<p>Restriction of access to premises</p> <p>Provided the party restricting access has a legal right to do so (i.e. is the owner or tenant of the premises) then the restriction of access to a premises is permissible.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>Provided the party restricting access has a legal right to do so (i.e. is the owner or tenant of the premises) then restricting access to certain areas of the premises is permissible.</p> <p>Physical screening (on entry/exit)</p> <p>Such screening is typically only undertaken at the entrances to government or commercial buildings.</p> <p>Prohibition of removal of data from the premises (hard-copy)</p> <p>Information and documents created during an individual's employment belong to the employer and employees can be prevented from removing such data from the employer's premises. There are provisions within the new data protection laws in Malaysia, however. Employers are also protected by Malaysia's involvement in the Patent Cooperation Treaty 2006 and the national legislations on patents, trademarks, copyright and industrial design.</p> <p>Prohibition of removal of data from the premises (electronic)</p> <p>See above.</p> <p>Visual surveillance (CCTV or other cameras), either overt or covert</p> <p>CCTV is commonly used in Malaysia in public spaces such as lifts, offices or shops. This also covers places of work and council authorities use it for public safety and crime prevention. Covert surveillance of employees in the workplace is not permitted, especially if it infringes a citizen's civil liberties.</p>

		<p>Overt monitoring of access to IT and other equipment</p> <p>IT equipment (such as computers and servers) and email can be monitored by an employer. There is no privacy legislation prohibiting such measures but it is preferable that the employer makes it known to all employees that such measures are being taken, and this may form part of the employment contract.</p> <p>Covert monitoring of access to IT and other equipment</p> <p>See above.</p> <p>Reporting hotlines (anonymous)</p> <p>There is no legislation prohibiting the use of reporting hotlines in Malaysia. These are commonly used by employers in Malaysia both internally and externally with customers. The procedures for receiving anonymous/confidential reports through such hotlines are usually communicated by employers to employees via corporate governance and HR policies.</p> <p>Reporting hotlines (confidential)</p> <p>See above. Confidential hotlines are preferred to anonymous hotlines. In addition, it is good practice for a company to disclose the identity of the organisation manning its hotline should this be a third party.</p> <p>Use of alerts/automated warning systems to identify unusual employee behaviour (out of hours activities, duplicate payments)</p> <p>These systems are available to employers in Malaysia should they wish to use them.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>Monitoring of communications is permissible, provided the medium of such communications belongs to the employer (i.e. work computer or telephones). Preferably, the organisation should inform employees that monitoring procedures may be carried out and this should be contained in the employment contract.</p>
4.8	<p>Formal investigations</p>	<p>Is there a licensing regime covering investigators?</p> <p>The establishment and activities of private investigators is regulated by the Private Agencies Act 1971 (amended up to 2006).</p> <p>Physical surveillance (overt or covert)</p> <p>Covert surveillance is illegal unless an authority or employer is given a licence for the purpose of monitoring an employee to see if he or she is involved in any unlawful activity.</p> <p>Electronic surveillance (e.g. tracking devices)</p> <p>No specific laws prohibit the use of electronic surveillance devices (overt and covert) by the police and licensed private investigators.</p>

Visual and communication surveillance (using cameras, video or CCTV)

Covert surveillance is illegal unless an authority or employer is given a licence for the purpose of monitoring an employee to see if he is involved in any unlawful activity.

Communication intercept (including oral, written and electronic communication including bugging devices)

Many organisations in Malaysia, such as government departments and leading financial firms, maintain tape recordings of their employees' telephone conversations as a matter of routine. The reasons for such recording will depend on the role but are usually for regulatory compliance or training purposes. Organisations that undertake this practice will generally notify employees of the use of recording and will explain the rationale for its use.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

For private investigations, it is possible to carry out computer or database surveillance if the equipment belongs to the organisation.

Formal interviews of staff

Across Malaysia, only the police and relevant government authorities have the powers to demand interviews for the purposes of a criminal investigation under the law. Interviews undertaken by any other party (e.g. the employer) for the purposes of investigation are considered voluntary and would require consent from the individual in question. An organisation's HR policies may provide for the mandatory assistance of an employee (either through interviews or physical searches) in an internal investigation.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

Financial transactional data and credit card activity are not available to third parties under the **Central Bank of Malaysia Act 2009** and the **Financial Services Act 2013**.

However, organisations that deem it necessary to monitor financial transaction data and credit card activity of their employees would provide for such measures under their HR policies and employment contract. Monitoring of building access logs and computer access logs is permissible as long as the building and equipment belong to the employer.

Search and seizure of evidence, whether electronic or physical (overt or covert)

Under Part 11 (ss 39–50) of the **Occupational Safety and Health Act 1994** enforcement and investigations that involve search and seizure by enforcement officers and employers are permissible should there be sufficient proof and just cause.

		<p>Is it either usual or necessary to involve the police in investigations?</p> <p>It is necessary to involve the police as soon as possible if there is a suspicion that a criminal offence has been committed.</p> <p>However, it is usual for employers to either carry out internal investigations or engage third parties (such as forensic accountants or private investigators) to perform investigations in commercial cases to establish prima facie evidence before making such a report to the police.</p> <p>Where matters involve internal disciplinary matters or corporate governance issues, there is no need to involve the police.</p> <p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>In Malaysia, involving law enforcement authorities depends on whether there is sufficient prima facie evidence to lodge the case. This is especially relevant in commercial cases where the authorities expect an organisation to undertake its own investigations (either on their own or through an independent third party) to gather the facts and <i>prima facie</i> evidence before lodging any complaint.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>There is an obligation under Criminal Procedures Code for all members of the public, including employers, to report crimes to the relevant magistrate or law enforcement authority.</p> <p>Section 4 of the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 is dedicated to the reporting responsibilities of organisations and the authorities.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

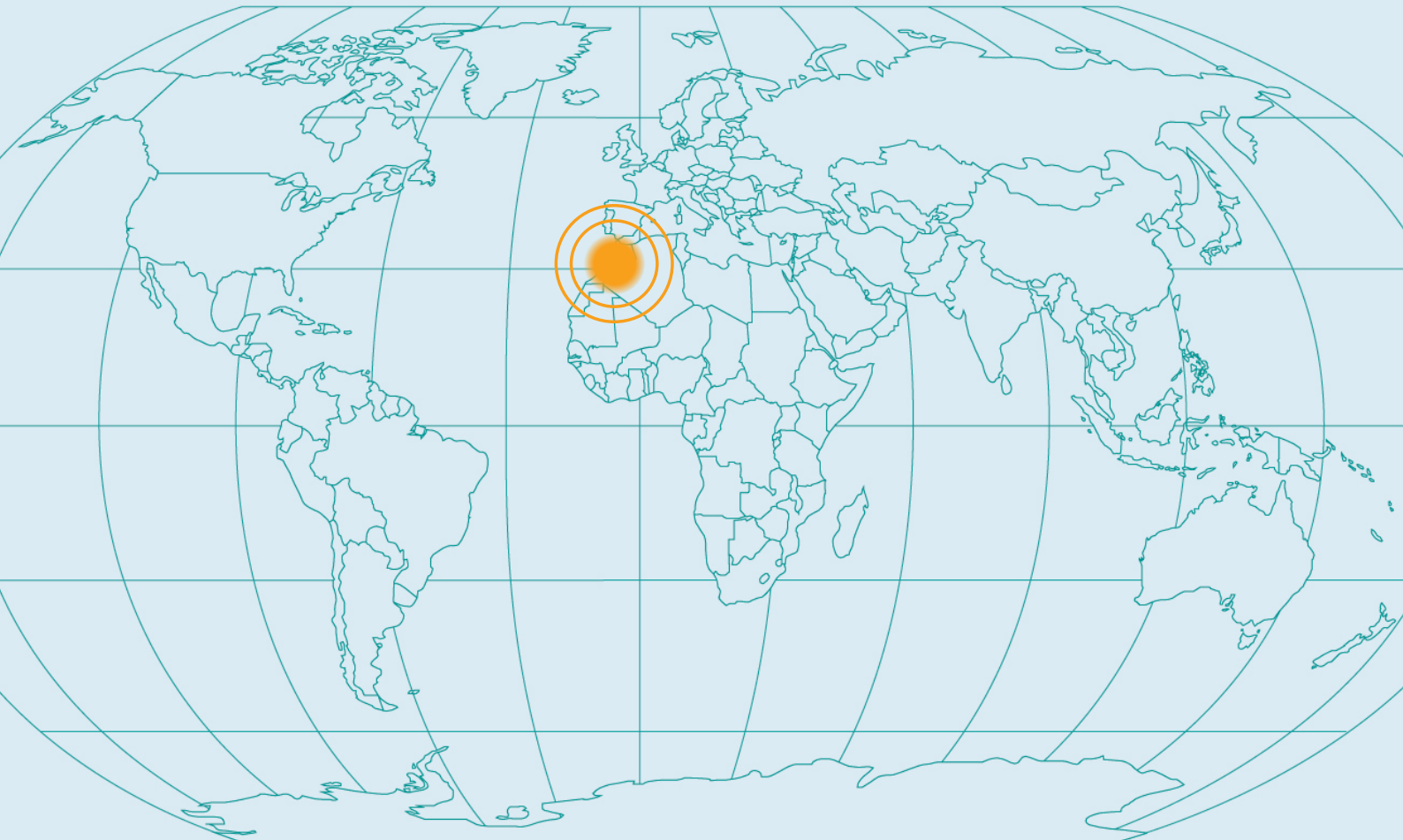
CPNI

Centre for the Protection
of National Infrastructure

SECURITY **WATCHDOG**
Part of Capita plc

Morocco

Personnel Security in Offshore Centres



Morocco

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

<p>1</p>	<p>Introduction</p>	<p>Morocco has one of the strongest economies in Africa. It is strategically located for Europe making it an ideal outsourcing destination, especially amongst French companies whose language it shares. Morocco has grown over the past few years making it the outsourcing destination 26th ranked in the world and the 3rd in Africa, and rising assuredly. Outsourcing to Morocco involves both business process and other forms of outsourcing.</p> <p>Morocco is located in the northern part of the Sahara. Owing to the European influence many people in the country can communicate in English. The use of the English language provides a good communication medium between outsourcing firms and their customers and favours outsourcing of business projects that require to be documented in English.</p> <p>The availability of a cheap labour pool has also contributed greatly to the rise of outsourcing to Morocco. This is as a result of a high population growth rate, which has led to high unemployment hence providing cheap and competent labour.</p> <p>Morocco has a good education system based on career development and this system has helped to equip students with the skills required in the outsourcing market. The education system has also led to improvement in research and innovation. Scientific and technological advances have gone a long way to promote outsourcing to Morocco.</p> <p>The Moroccan government has invested money to ensure that Morocco emerges as a top outsourcing destination. This investment is in the form of subsidies and tax relief to companies that have outsourced. This has driven down the price of outsourcing services making outsourcing to Morocco cheap and affordable. In a bid to reduce unemployment the Moroccan government has also embarked on a massive campaign to market outsourcing to Morocco to the outside world.</p> <p>Morocco is well connected by air, water and road transportation. This works well to provide a good base for overseas outsourcing. The other key infrastructure aspect is communications. Morocco has a well-linked communication network and it is installing fibre-optic internet connectivity to provide both online and telecommunication links with outsourcing countries.</p> <p>The main concentration of outsourcing companies in Morocco is in the corridor between Casablanca and Rabat and is estimated to be employing over 55,000 people.</p> <p>Moroccan laws enhance data and property security and protect outsourcing clients from possible theft of their data and inventions.</p>
<p>2</p>	<p>Personnel security measures during recruitment</p>	

2.1	Culture of screening	<p>Pre-employment screening is not well received by the majority of Moroccans since questioning an individual's background is generally viewed as unnecessary and verging on the offensive. Despite this cultural and religious attitude, pre-employment screening is an emerging practice, especially within the major cities and offshoring locations as more western and international businesses establish operations in Morocco.</p> <p>The globalisation of international corporate policies means that the recruitment policies of companies become aligned across their operations and this means that pre-employment screening is being adopted in Morocco.</p> <p>Verifying an individual's background is largely documentary in nature with a reliance on prospective employees supplying employers with the required documentation. Referencing directly with previous employers or institutions is only carried out by larger companies.</p> <p>Attitudes towards pre-employment screening have a secondary effect on the typical timeframes in which it can be carried out. As its value is seen to be minimal by many employers and institutions response times can be considerably slower than other countries.</p>
2.2	Major laws and regulations applying to pre-employment screening	<p>Following the 2011 protests Morocco enacted a new Constitution (French) which was approved by referendum in July 2011. The constitution recognises freedom of association, the right to strike and the freedom to join unions. Although the new constitution is an improvement on the previous one the country remains a kingdom, power resides with the king and civil liberties are not central to the reform.</p> <p>The current Labour Code was established by <i>Dahir</i> (royal decree) in 2003. It regulates employment relations, working age, maternity leave, working hours, occupational safety and health, wages, trade union and employers' representation and works councils. It also regulates settlement of collective labour disputes and establishes the rules.</p> <p>The <i>Dahir</i> establishing the Labour Code is the most important labour legislation. Several other laws regulate and set standards and restrictions for the labour market. Most of them are also <i>Dahirs</i> and several were repealed by the Labour Code.</p> <p>Although the new Constitution now allows individuals to join independent trade unions and the Labour Code specifically prevents employers from persecuting employees that do, Morocco is not heavily influenced by trade unions with only 15% of waged workers belonging to one of 5 national unions.</p> <p>Personal data protection is governed in Morocco by Law no. 09-08 of 18 February 2009 (the 'Law' – French only) relating to the protection of individuals with respect to the processing of personal data and by its implementation Decree no. 2-09-165 of 21 May 2009 (the 'Decree').</p>

		<p>The national data protection authority is the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel ('CNDP') (National Control Commission for the Protection of Personal Data) which was established in 2011 when the law was officially recognised by the international community.</p> <p>The main principles of the Law are largely aligned with the European Data Directive as regards fair and lawful processing of personal data, although punitive fines are minimal and companies are not legally required to appoint a Data Protection Officer. This alignment is deliberate so as to attract outsourcing or offshoring investment from Europe and Internationally.</p>
3	Pre-employment checks	
3.1	Identity check	<p>As it is a legal requirement to possess one, Moroccan citizens will mostly present their National Identity Card (Carte d'Identité Nationale). Since 2008 all citizens have been issued with a biometric card called the Electronic National Identity Card (NIEC). The NIEC replaces the need to issue a birth certificate, certificate of residence, certificate of life and certificate of nationality in all procedures for which these documents must be provided, as these data are captured on the card.</p> <p>As an alternative Moroccan citizens may present their passport, birth certificate (in Arabic and in French) or family book (L'Etat Civil).</p> <p>Foreign nationals who have residency in Morocco will present their foreign passport with supporting residency and working visa documentation.</p>
3.2	Checks on eligibility to work	<p>In Morocco employers seeking to employ foreign nationals must obtain a work permit from the Ministry of Employment before the foreigner can commence work.</p> <p>Employers should check visa entitlements of foreign nationals when checking their identity.</p>
3.3	Residency checks	<p>Foreign nationals must register with the police and apply for a resident's permit (Certificat d'Immatriculation). Applications should be submitted to the Bureau des Etrangers of the Préfecture de Police or Commissariat Central, in major cities, and to the Gendarmerie in small towns and villages.</p> <p>There are eight categories of Moroccan residence permit. Employers are most likely to be presented with two types for the purposes of employment:</p> <ul style="list-style-type: none"> • Employment contract approved by the Ministry of Labour or • Contractual. <p>Employers should ensure that residency status is checked for non-Moroccan nationals.</p>

<p>3.4</p>	<p>Criminal record checks</p>	<p>Name of certificate Casier Judiciaire (Bulletin III) or Fiche Antropométrique.</p> <p>Department that holds records Ministry of Justice.</p> <p>Where to apply within country Ministry of Justice, Place Mamounia, Rabat Website: www.justice.gov.ma</p> <p>How to apply within country Applications can be made in person at the Ministry of Justice, Place Mamounia, Rabat. Applications can also be made on line at the following address: http://casierjudiciaire.justice.gov.ma</p> <p>Who can apply Citizens and non-citizens can apply through the Ministry of Justice. Citizens can also apply to the Président du Tribunal de Premier Instant at their place of birth.</p> <p>Cost, payment and turnaround The cost of obtaining a Casier Judiciaire (Bulletin III) or Fiche Antropométrique is DH10. Turnaround times vary from three to five days depending on the method of delivery selected.</p> <p>Legislation Further information on overseas criminal records in Morocco can be found at www.justice.gov.ma. Information on overseas criminal records in other countries can be obtained from the CPNI guidance on <i>Overseas Criminal Record Checks</i> which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>
<p>3.5</p>	<p>Education checks</p>	<p>There are only 14 leading universities in Morocco servicing the major cities and regions in the country. Morocco has seen an increase in Business Administration degrees over Engineering and Medicine in recent years.</p> <p>Education checks are often required by employers to establish that a prospective employee has attended the educational establishments claimed.</p> <p>Most prospective employees will present their degree certificates as proof of their education and university attendance. Employers should be alert to the risk of fake establishments and/or fake qualifications issued by such establishments. Where the educational establishment is not well known, it may be necessary to undertake additional checks to verify its authenticity.</p>

		<p>Applications for references must typically be made in writing and provide all known information, e.g. full name, date of birth, subject of study and an explanation of the reason for the request. However, whether any information will be disclosed depends on the discretion of the university or college.</p> <p>Typical information provided is dates of joining and leaving the educational institution (school, college or university), subject of study, courses (college, university), degree and final mark.</p> <p>It is considered culturally unacceptable to ask questions about an individual's character, so character references should not be requested from tutors.</p> <p>It would be customary for the requestor to initially speak with the referee or institution to introduce the reference request instead of sending it to them without advance explanation.</p>
3.6	Qualification checks	<p>Verification of professional qualifications is used as part of the pre-employment screening process in Morocco for those roles that require a particular qualification.</p> <p>Typical information provided is dates of joining and leaving the educational institution or professional body, membership status (professional body), status and type of qualification. In many cases, all known information has to be provided. The institution will usually confirm this information although it might not volunteer any data.</p> <p>Generally, questions regarding the character of an individual will not be answered by professional institutions.</p> <p>Application is made directly to the professional body concerned. Most educational establishments have standard processes for dealing with reference enquiries. The consent of the individual is generally required and recommended. The information may be sometimes available online for common qualifications, but generally professional bodies in Morocco do not publish online directories.</p> <p>It is also important to verify that the individual is an active member of a professional body and has not left nor been ejected from membership.</p>
3.7	Employment references	<p>Questioning the genuineness of an individual's background as presented to an employer is culturally sensitive in Morocco, so care should be taken when conducting employment checks.</p> <p>Previous employers might provide references upon direct request. These may confirm basic information such as dates of employment, positions held and reason for leaving. They will rarely include character references or personal comment as culturally this is unacceptable. Also, most employers will not provide information on salaries, sickness record or parental leave.</p> <p>Applications are generally made in writing to the employer concerned and a telephone call to introduce the request is often considered courteous in Moroccan culture.</p>

		<p>Some prospective employees may present certificates of employment from previous employers as proof of their work history.</p> <p>As employment referencing is not common practice in Morocco a dominant methodology (referencing or Labour Book) has not emerged.</p> <p>An employee must give consent to obtaining such information under the data protection legislation.</p>
3.8	Financial/ credit checks	<p>Financial/credit checks are very rarely carried out for employment purposes in Morocco and are generally used only for very senior roles or those that involve access to financial systems or controls (in particular, in the banking and government sector). They are not commonly carried out outside the government or financial sectors and would be considered excessive in most other sectors.</p> <p>There is no specific provision within the Labour Code permitting or prohibiting the use of financial checks on employees. Morocco is not considered a credit society so its credit infrastructure is not sufficiently developed to support public credit files available outside the banking community.</p>
3.9	Substance abuse screening	<p>Historically, Morocco has had a significant drug issue, in terms not only of consumption within the Kingdom but also of export into Europe and internationally. Despite this, drug testing in the workplace is rarely carried out outside high-risk roles.</p> <p>Alcohol testing is not culturally well perceived since it is strictly forbidden to drink alcohol in a Moroccan company. The consequence of reporting for duty under the influence of alcohol is dismissal without notice, as this will be regarded as gross misconduct.</p>
3.10	Occupational health checks	<p>Industrial and commercial institutions hiring more than 50 workers have to organise work medical services.</p> <p>This work medical service is also imposed on institutions hiring fewer than 50 workers when their activity is likely to cause an occupational illness. The cost of the medical service is met by the employer.</p>
4	Personnel security measures during employment	
4.1	Legal requirements	<p>The current Labour Code 2003 remains the dominant legislation governing the ongoing relationships and responsibilities between employers and employees. It regulates employment relations, working age, maternity leave, working hours, occupational safety and health, wages, trade union and employers' representation and works councils. It also regulates settlement of collective labour disputes and establishes the rules.</p>

		<p>The main legislative documents on occupational safety and health in Morocco include the Labour Code and Decision 93-08 of 12 May 2008. Other legislative documents regulate particular hazards, covering large sectors such as agriculture, services, and the public sector, with a special emphasis on the proper maintenance of facilities. Occupational health and safety legislation is specific, but the law does not specify a competent national authority for safety and health at work. There have been plans laid out by government to create a Health and Safety Institute but these remain to be put into force and occupational safety remains embedded in the Labour Code.</p> <p>The data privacy laws Law no. 09-08 of 18 February 2009 apply to all employers throughout the term of an individual's employment with them. Employers must ensure that they only process employees' personal data lawfully, with specific purpose and always with the employee's consent. Failure to do so could result in prosecution by the CNDP and a statutory fine, although there are few precedents of prosecution under this law in Morocco.</p>
4.2	Laws governing the rights of the employee or employer	<p>The Labour Code 2003 remains the dominant legislation governing the ongoing relationships and responsibilities between employers and employees.</p> <p>The Moroccan Constitution provides equal treatment under the law for its citizens and guarantees them the right to freely choose work, equality in gaining employment, the right of freedom of association and the right to strike.</p>
4.3	Local legislation that specifically governs the rights of the employer	<p>All employers must comply with the Labour Code 2003.</p> <p>The employer must also register itself as well as its salaried employees and apprentices with the National Fund for Social Security (Caisse Nationale de Sécurité Sociale, CNSS).</p> <p>Moroccan employers can join the Confédération Générale des Entreprises du Maroc (CGEM) – General Confederation of Moroccan Enterprises. The CGEM is the main employers' organisation. It includes large industrial and commercial companies as well as small and medium-sized enterprises.</p>
4.4	Local legislation that specifically governs the rights of the employee	<p>The Moroccan Constitution provides equal treatment under the law for its citizens and guarantees them the right to freely choose work, equality in gaining employment, the right of freedom of association and the right to strike.</p> <p>Occupational illnesses are covered by provisions similar to the law on occupational accidents.</p>

4.5	<p>What avenues are open to employees who seek to challenge an employer's use of security procedures?</p>	<p>The Ministry of Employment, Social Affairs, and Solidarity is the government agency responsible for employment and protection of workers' rights. The Department for the Social Protection of Workers develops measures and actions to provide workers with social safety-net protection.</p> <p>Workers can appeal their case to the Department should they believe that their dismissal was unjust.</p>
4.6	<p>What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?</p>	<p>See Section 4.5 above.</p>
4.7	<p>Availability of security measures</p>	<p>Restriction of access to premises</p> <p>Provided the party restricting access has a legal right to do so (i.e. is the owner or tenant of the premises) then the restriction of access to premises is permissible.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>Provided the party restricting access has a legal right to do so (i.e. is the owner or tenant of the premises) then restricting access to certain areas of the premises is permissible.</p> <p>Physical screening (on entry/exit)</p> <p>Such screening is typically undertaken only at the entrances to government buildings and utilises scanning technology rather than physical touch.</p> <p>Prohibition of removal of data from the premises (hard-copy)</p> <p>Information and documents created during an individual's employment belong to the employer and employees can be prevented from removing such data from the employer's premises. There are provisions within the data protection laws about the handling of sensitive personal data and these apply to the workplace.</p> <p>Prohibition of removal of data from the premises (electronic)</p> <p>See above.</p>

Visual surveillance (CCTV or other cameras), either overt or covert

CCTV is not extensively used in Morocco, although when it is used this is normally for security and safety reasons. There is seemingly no specific legislation prohibiting the use of CCTV in the workplace and this could be required under the health and safety provisions of the Labour Code 2003.

The data protection law in Morocco now places conditions on employers to ensure that they do not start processing sensitive information on individuals unlawfully and without the individual's explicit consent. For this reason employers will need to at least notify employees on the use of CCTV in the workplace.

Covert use of CCTV in the workplace could be permissible if there was active suspicion of criminal activity.

Overt monitoring of access to IT and other equipment

IT equipment (such as computers and servers) and email can be monitored by an employer. There is no privacy legislation prohibiting such measures but it is preferable that the employer makes it known to all employees that such measures are being taken, and this might form part of the employment contract.

Covert monitoring of access to IT and other equipment

See above.

Reporting hotlines (anonymous)

There is no legislation prohibiting the use of reporting hotlines in Morocco although these are not commonly used. The procedures for receiving anonymous/confidential reports through such hotlines are usually communicated by employers to employees via corporate governance and HR policies.

Reporting hotlines (confidential)

See above. In addition, it is good practice for a company to disclose the identity of the organisation manning its hotline should this be a third party.

Use of alerts/automated warning systems to identify unusual employee behaviour (out of hours activities, duplicate payments)

These systems are available to employers in Morocco should they wish to use them.

Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)

Monitoring of communications is permissible, provided the medium of such communications belongs to the employer (i.e. the work computer or telephones). Preferably, the organisation should inform employees that monitoring procedures may be carried out and this should be contained in the employment contract.

4.8

Formal investigations

Is there a licensing regime covering investigators?

There is no specific licensing regime or legislation covering private investigators in Morocco, although there are some specialist private investigation agencies present in the country and many international agencies will work in Morocco.

In September 2013, the anti-censorship organisation Article 19 examined Draft Law No 31.13 on the Right of Access to Information (the 'Draft Law'). Their review and recommendations on the draft legislation may have implications for the private investigation industry. Article 19 recommends that the Draft Law should clearly state the powers of the Commission, specifically the powers of investigation, the right to order the production of evidence, to examine any information disclosure of which is being sought and to compel witnesses to testify; and that Article 32 (previously Article 35) of the Draft Law, which threatens civil servants with criminal sanctions for releasing information, should be deleted.

Physical surveillance (overt or covert)

There are no specific laws that prohibit physical surveillance (overt and covert) by the police and licensed private investigators.

Electronic surveillance (e.g. tracking devices)

There are no specific laws that prohibit the use of electronic surveillance devices (overt and covert) by the police and licensed private investigators.

Visual and communication surveillance (using cameras, video or CCTV)

There is seemingly no specific legislation prohibiting the use of CCTV in the workplace and this could be required under the health and safety provisions of the Labour Code 2003.

Employers will need to at least notify employees of the use of CCTV in the workplace.

Covert use of CCTV in the workplace could be permissible if there was active suspicion of criminal activity.

Communication intercept (including oral, written and electronic communication including bugging devices)

Some organisations in Morocco, such as government departments or leading financial firms, may maintain tape recordings of employees' telephone conversations as a matter of routine. The reasons for such recording will depend on the role but are usually for regulatory compliance or training purposes. Organisations who undertake this practice will generally notify employees of the recording and will explain the rationale for its use.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

For private investigations, it is possible to carry out computer or database surveillance if the equipment belongs to the organisation. Police enforcement authorities can exercise a greater set of powers as part of formal investigations.

Formal interviews of staff

Normally in Morocco, only the police and relevant government authorities have the powers to demand interviews for the purposes of a criminal investigation under the law. Interviews undertaken by any other party (e.g. employer) for the purposes of investigation are considered voluntary and would require consent from the individual in question. An organisation's HR policies may provide for the mandatory assistance of an employee (either through interviews or physical searches) in an internal investigation.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

Monitoring of building access logs and computer access logs are both permissible as long as the building and equipment belong to the employer.

The monitoring of email, website activity and credit card logs is not common in Morocco, although large corporates and especially multinationals may carry out such activities as part of their global standards and policies.

Search and seizure of evidence, whether electronic or physical (overt or covert)

Employers could seize evidence on their premises should there be sufficient cause and especially if this is carried out as a means of securing their own assets. Any seizure of property or assets off-site must be carried out by the relevant police authority.

Is it either usual or necessary to involve the police in investigations?

It is necessary to involve the police as soon as possible if there is a suspicion that a criminal offence has been committed.

However, it is usual for employers to either carry out internal investigations or engage third parties (such as forensic accountants or private investigators) to perform investigations in commercial cases, to establish prima facie evidence before making any report to the police.

Where matters involve internal disciplinary matters or corporate governance issues, there is no need to involve the police.

The severity of the crime will determine whether employers involve the Moroccan Police (Sûreté Nationale) or the Royal Police (Gendarmerie Royale). The Royal Police now have counter-terrorism responsibilities.

		<p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>In Morocco, involving law enforcement authorities depends on whether there is sufficient <i>prima facie</i> evidence to lodge a case. This is especially relevant in commercial cases where the authorities expect an organisation to undertake its own investigations (either on their own or through an independent third party) to gather the facts and prima facie evidence before lodging a complaint.</p> <p>In recent years Moroccan police authorities have suffered negatively from reports of abuse of individuals’ civil liberties.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>There is an obligation under the Constitution for all members of the public, including employers to report crimes to the relevant law enforcement authority.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

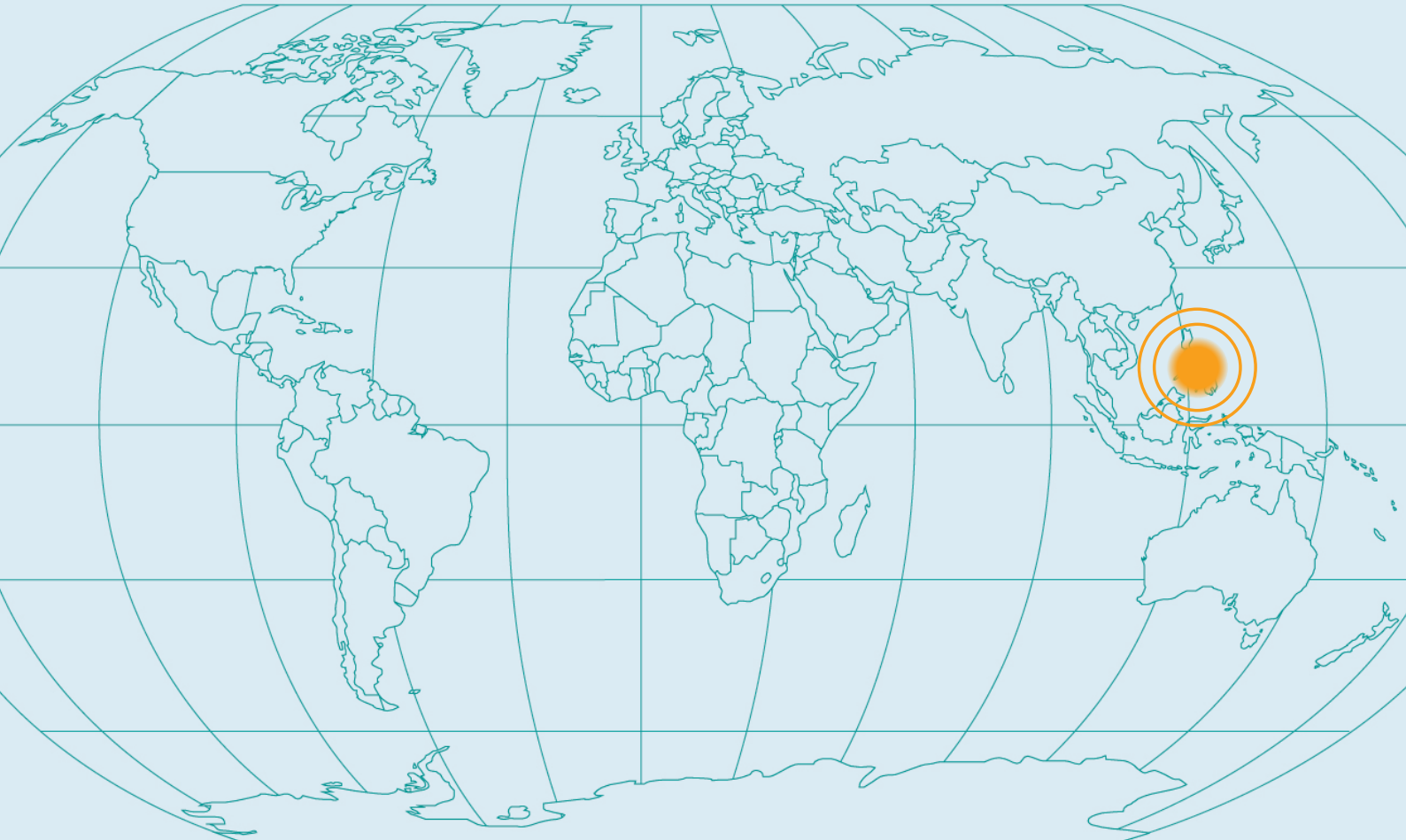
CPNI

Centre for the Protection
of National Infrastructure

SECURITY **WATCHDOG**
Part of Capita plc

Philippines

Personnel Security in Offshore Centres



Philippines

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1	Introduction	<p>The Philippines is one of the largest outsourcing centres in Asia and is ranked as one of the top ten outsourcing destinations in the world. As a former colony of both the United States and Spain, the country benefits from a large English- and Spanish-speaking population. It is also close to the United States, culturally, making it a popular destination for US companies seeking to establish offshore operations. The Philippines has high rates of literacy and particular skills in areas such as information technology. The country has a developed IT infrastructure. Outsourced operations in the Philippines include call centres, business process outsourcing (BPO) operations, IT support operations, medical data transcription services (for example, medical record transcriptions or interpretation of MRI scans, etc), art, animation and desktop publishing.</p> <p>The Constitution of the Philippines protects individuals’ rights to privacy. An employer’s rights are protected by legislation including the Electronic Commerce Act 2000, which imposes confidentiality over data, and the Banking Secrecy Act 1995.</p> <p>In 2012 the new Data Privacy Act, influenced by global legislation such as Directive 95/46/EC of the European Union and data protection laws in other Asia-Pacific countries, introduced stringent regulations regarding the handling of ‘sensitive personal information’ and established the National Privacy Commission (NPC) to implement and regulate the legislation. Data subjects were afforded new rights and the Act introduced sanctions for breaches of its rules including:</p> <ul style="list-style-type: none"> • fines and custodial sentences • deportation of non-Filipino citizens • preventing violating companies from processing personal data and • continuing liability of data controllers for personal information sent outside the Philippines or to intermediate processors.
2	Personnel security measures during recruitment	
2.1	Culture of screening	<p>In the Philippines pre-employment security screening measures are not used by all employers. Where they are used, they are usually applied to all levels of staff although enhanced screening measures may be applied for those staff with access to sensitive data. These would include taking up references with a person of suitable authority and integrity, to confirm the qualifications of the candidate.</p> <p>Employers in the Philippines must ensure that a prospective employee has the right to work in the country. Companies who take on staff without ensuring they have the right to work are liable to criminal prosecution. Right to work legislation is covered in the Labor Codes of the Philippines.</p>

2.2	Major laws and regulations applying to pre-employment screening	<p>A number of laws apply in the Philippines including:</p> <ul style="list-style-type: none"> • Section 1 of Article III of the Bill of Rights of the Constitution of the Republic of the Philippines sets out ‘the right of all the people to human dignity’ and ss 2 and 3 of the Article set out individuals’ rights to privacy, including rights in relation to privacy of papers and communications: see www.lexadin.nl/wlg/legis/nofr/oeur/lxwephi.htm for further information • Section 5 of the Bill of Rights sets out the legal requirement for the free exercise and enjoyment of religious beliefs without discrimination • Section 8 of the Bill of Rights sets out the rights of people to form unions for purposes not contrary to the law; in particular, employers should be aware of the need not to discriminate as part of the pre-employment screening process and • the Data Privacy Act 2012 regulates the handling of ‘sensitive personal information’ and imposes strict sanctions on individuals and companies in breach of the rules.
3	Pre-employment checks	
3.1	Identity check	<p>It is common practice in the Philippines to undertake identity checks on prospective employees. This includes checks on the family name, given name, date of birth, place of birth, nationality and parents’ names and address.</p> <p>Prospective employees will commonly provide one of the following proofs of identity:</p> <ul style="list-style-type: none"> • driver’s licence • passport • Social Security System ID (UMID) • Tax Identification Number • marriage certificate and/or birth certificate or • professional identification – Professional Regulation Commission (PRC) ID. <p>The PRC ID is obtained by professionals from the PRC. All professionals who have taken and passed examinations administered by the PRC are expected to register with it. This includes the following qualifications/ professions: Bachelor of Science (BS) in Accountancy; in Nursing; in Education; in Pharmacy; in Physical Therapy; in Engineering. Following registration, individuals are issued with the ID.</p> <p>If an official form of identification cannot be provided by the prospective employee, the individual may obtain an affidavit duly notarised by a lawyer affirming their identity.</p> <p>Forms of ID may be verified as follows:</p> <ul style="list-style-type: none"> • marriage/birth certificates are printed on special paper only used by the National Statistics Office and • other IDs are printed on cards that are specially supplied to issuing offices. Security features are embedded in the cards such as the logo, serial numbers, magnetic strip and signatures. <p>If there is doubt over the authenticity of ID, it is possible to call the issuing office to verify it.</p>

<p>3.2</p>	<p>Checks on eligibility to work</p>	<p>Non-Filipinos are required to hold a work permit or pre-arranged working visa before being employed in the Philippines. An Alien Employment Permit may be issued by the Department of Labor and Employment to authorise a foreign national to work in the Philippines.</p> <p>More information is available at http://immigration.gov.ph/ under 'Services'.</p> <p>The following professions may qualify for work permits/visas:</p> <ul style="list-style-type: none"> • professors and teachers in educational establishments • doctors and nurses • scientists • professionals and • other employees in banking, commercial, industrial, agricultural and other business enterprises. <p>Employers in the Philippines usually ask prospective employees to provide work permit documentation or present their Alien Certificate Registration (ACR) I-Card, if they hold one. The ACR I-Card is a microchip-based, credit-card-sized, identification card with biometric security features, issued to registered aliens and replacing the paper-based ACR. It is fraud and tamper-proof/resistant and contains the following data:</p> <ul style="list-style-type: none"> • personal information such as name, age, date of birth, place of birth, etc • photograph • date and status of admission • visa type including date granted and date of expiry • biometric information (two digitalised fingerprint templates) • signature • the numbers of the individual's: <ul style="list-style-type: none"> – Certificate of Residence (Immigrant Certificate of Residence or ICR) – Natural-Born Certificate of Registration (NBCR) – Certificate of Residence – Temporary (CRTV) – Certificate of Residence for Treaty Traders (CRTT) – Certificate of Residence for Temporary Students (CRTS) or – Certificate of Residence – Pre-arranged Employee (CRPE) • travel details and • details of payment of immigration fees. <p>More information about the ACR I-Card can be found at www.immigration.gov.ph/index.php/services/alien-registration/acr-i-card-issuance</p>
-------------------	---	---

3.3	Residency checks	<p>In the Philippines it is common practice to undertake residency checks as part of the pre-employment security screening process. Prospective employees are generally required by employers to provide a <i>barangay</i> (community) Clearance Certificate and/or a Residence Certificate (CEDULA). The <i>barangay</i> Clearance Certificate is signed by the local community chairman, and states:</p> <ul style="list-style-type: none"> • that the individual is a resident of the local community • the length of time the individual has resided in the community and • the name by which the individual is known. <p>Employers may require prospective employees to provide a sketch map showing the location of their residence, including brief directions how to reach it, to facilitate background checks.</p> <p>The certificate should bear the <i>barangay's</i> dry seal and the signature of the authorised individual, who is generally the <i>barangay</i> chairman. The employer can telephone the <i>barangay</i> office to verify the identity of its chairman, or if important, send someone to the office to personally verify the validity of the certificate.</p>
3.4	Criminal record checks	<p>Name of certificate</p> <p>National Bureau of Investigation (NBI) Clearance Certificate</p> <p>Department that holds records</p> <p>National Bureau of Investigation, NBI Building, Taft Avenue, Ermita, Manila, Philippines 1000.</p> <p>Where to apply within country</p> <p>NBI Clearance Building, United Nations Avenue, Ermita, Manila, Philippines 1000.</p> <p>Telephone: +63 (0) 523 8231 Fax: +63 (0) 526 1216 Email: nbiclearance@nbi.gov.ph Website: www.nbi.gov.ph</p> <p>A list of all of the NBI offices in the Philippines is available on the NBI website: www.nbi.gov.ph/field_offices.html.</p>

How to apply within country

In person

First-time Applications

- Complete the application form online at <http://nbi.njis-ph.com/> or obtain a form from one of the local offices.
- Pay the fee.
- Individual is photographed and assigned a photograph number.
- Individual presents a valid form of identification (e.g. passport, driver's licence, or PRC ID).
- Fingerprints are taken and printed on a fingerprint card.
- The NBI Clearance is printed and dry-sealed (clearance issued without the dry seal is invalid) prior to releasing.

Renewal applications within the Philippines (when a certificate has expired after its 12-month validity)

- The individual should provide the original of their previous NBI Clearance certificate.
- Applications for renewal can also be carried out by an authorised representative.
- This requires the representative to provide the original of the individual's previous clearance certificate and a recent, standard passport-size photograph.

There must have been no significant changes to the status of the individual (i.e. name, marital status etc.). If this is the case, a new application may be required.

Who can apply

Individuals only; third parties (with consent) can apply for renewals.

Cost, payment and turnaround

Cost

PHP 115 payable in cash.

Turnaround

Turnaround time varies depending on the NBI office conducting the application, but is between 30 minutes and 7 days.

There is no fast-track service available.

Legislation

There is no legislation that specifically governs the disclosure of criminal records. However, the NBI has internal policies and procedures that govern the disclosure of criminal records.

Further information can be obtained from the CPNI guidance on Overseas Criminal Record Checks which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/

3.5	Education checks	<p>Prospective employees are usually required to provide a copy of their diploma and a transcript of records. They may also be required to provide a certificate from the school they attended stating they are a graduate of that school, the title of the course completed and the date of graduation.</p> <p>Schools in the Philippines commonly issue Certificates of Good Moral Character, which are required by prospective employers. Certificates should bear the school's dry seal and be signed by an authorised individual. They certify a person's behaviour or performance at school. A separate process is initiated to confirm a person's moral character. Verification of the authenticity of such a certificate can be ascertained by contacting the school.</p> <p>For character references, prospective employees are asked to provide the names, addresses and contact numbers of at least three referees who are not relatives.</p>
3.6	Qualification checks	<p>Verification of qualifications (academic or professional) is regularly undertaken as part of pre-employment screening. Most educational establishments have standard processes for dealing with reference enquiries. The consent of the individual is generally required. Typical information provided includes joining and leaving dates and membership status (professional bodies).</p> <p>Recommendation letters may generally be obtained from the educational institution or from a tutor who knows the individual.</p> <p>Most professional bodies issue original copies or an authenticated/certified true copy of any document requested.</p> <p>Fake documentation is widespread within the Philippines and a large proportion of employment candidates lie about or exaggerate their qualifications.</p>
3.7	Employment references	<p>Prospective employees may be required to submit a certificate of employment from their previous employer. If the employer providing the reference is not from a well-known company it may be necessary to undertake further enquiries to establish the validity of the reference.</p> <p>Character references from previous employers</p> <p>In the Philippines the prospective employee is usually required to provide at least three character references.</p> <p>Previous employers might not always provide character references and often limit information to dates of employment and reason(s) for leaving.</p> <p>Character references from persons of standing in the community</p> <p>These may include police officers, public officials or professionals who have known the individual for a period of more than three years.</p> <p>Verification would be undertaken directly with the individual referees. Care should be taken to ensure that these individuals are independent of the prospective employee (e.g. are not family members).</p>

3.8	Financial/ credit checks	<p>It is not common practice to run financial or credit checks on prospective employees in the Philippines, except in the banking industry.</p> <p>The Bankers Association of the Philippines (BAP) Credit Bureau Inc maintains the NFIS (Negative File Information System). It is a computerised information system launched by the Bureau in 1992 that provides member banks with data about clients with adverse records. At present the system is operated and maintained by the Bureau and is accessible for inquiries through registered users from the different BAP member banks.</p> <p>The NFIS maintains over four million records of credit cards cancelled for mishandling, current accounts closed by the banks for improper usage, loans classified as foreclosed, litigation, accounts written off and court cases related to sums of money. It may be accessed through the internet and enquiries can be automatically requested within five minutes.</p>
3.9	Substance abuse screening	<p>In the Philippines substance abuse screening is not a widespread part of the pre-employment screening process. Where it is used, it may be part of ongoing screening: either random screening or where suspicions arise during the course of employment.</p> <p>Whilst there are no legal or cultural restrictions on substance abuse screening, it is likely to be a sensitive topic and normally would only be applied in specific situations (for example, where the employee presents a heightened level of risk to the employer because of his or her prospective position or level of access).</p>
3.10	Occupational health checks	<p>Occupational health checks may be used as part of the pre-employment screening process in the Philippines and may include:</p> <ul style="list-style-type: none"> • dental check • eye check • laboratory test (chest X-ray, urinalysis, stool examination) or • physical examination performed by a doctor.
4 Personnel security measures during employment		
4.1	Legal requirements	<p>In the Philippines the principal legal measures relevant to ongoing personnel security measures are as follows:</p> <ul style="list-style-type: none"> • Sections 2 and 3 of Article III of the Bill of Rights of the Constitution of the Republic set out an individual’s right to privacy and are relevant to the conduct of ongoing personnel security measures • Republic Act No. 4200, An Act to Prohibit and Penalize Wire Tapping and other related Violations of the Privacy of Communication, and for other Purposes, reinforces individuals’ rights to privacy of communications under Article III, s. 3(1) of the Constitution • the Data Privacy Act 2012 has introduced the concept of individuals’ rights to their personal information – any handling of such data must be undertaken with care following the newly established regulations

		<ul style="list-style-type: none"> • the confidentiality of bank records is protected by the Bank Secrecy Act 1995 and the Secrecy of Bank Deposits Act; the Anti-Money Laundering Act 2001 provides exceptions to these Acts for reporting money laundering concerns and • the Electronic Commerce Act 2000 (also known as Republic Act No. 8792) mandates a fine and a prison term for unlawful and unauthorised access to computer systems. Section 31 of the Act states that only persons with a lawful right to the data should have access to it; s. 32 imposes an obligation of confidentiality on persons receiving electronic data pertaining to other persons.
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	In the Philippines the rights of the employer are governed by the Labor Codes of the Philippines. These are in a decree instituting a labour code that revises and consolidates labour and social laws to afford protection of labour, to promote employment and human resources development and to ensure industrial peace based on social justice.
4.4	Local legislation that specifically governs the rights of the employee	<p>The Labor Codes of the Philippines (noted above) also govern the rights of employees.</p> <p>In addition, trade unions exist in the Philippines. Article III of the Bill of Rights of the Constitution of the Republic governs the rights of individuals, including those employed in the public and private sectors, and allows the formation of unions, associations or societies.</p>
4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	<p>Individuals may bring complaints against their employer under the Labor Codes of the Philippines. In addition, many employers have established complaints procedures, which may involve local trade union representatives to represent employees.</p> <p>Action may also be brought under the Data Privacy Act 2012, where an individual believes that personal data has been misused.</p>
4.6	What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?	<p>Employees seeking to challenge dismissal may bring a claim for unfair dismissal to the National Labor Relations Commission under the Department of Labor and Employment. The labour arbiters have jurisdiction over the case. Detailed guidance is available at www.dole.gov.ph.</p> <p>Where an employee is subject to disciplinary proceedings there are standard disciplinary, dismissal and grievance processes that must generally be followed. These include verbal warnings, written warnings, suspension and termination. Serious issues normally involve formal investigations in which the employee is invited to give his or her account of the situation.</p>

<p>4.7</p>	<p>Availability of security measures</p>	<p>Restriction of access to premises</p> <p>There are no specific legal restrictions concerning access to premises. Generally this is controlled through the issue of access cards to authorised personnel. Biometric access controls are rarely used, for cost reasons.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>See above.</p> <p>Physical screening (on entry/exit)</p> <p>See above.</p> <p>Prohibition of removal of data from the premises (hard-copy)</p> <p>The E-Commerce Act 2000 (Republic Act No. 8792) governs commercial and non-commercial transactions and provides penalties for unlawful transactions and other situations. For further information see www.lawphil.net.</p> <p>Prohibition of removal of data from the premises (electronic)</p> <p>Electronic data is also covered by the E-Commerce Act (see above).</p> <p>Visual surveillance (CCTV or other cameras), either overt or covert</p> <p>Visual surveillance is a commonly used measure in the Philippines, particularly in financial institutions. In the Philippines rights to privacy are safeguarded under Article III of the Bill of Rights, Section III of the Constitution of the Philippines and the Data Privacy Act. However, visual surveillance is generally restricted to common areas (such as the office lobby, elevators and office perimeter). It is not generally used in private offices or meeting rooms.</p>
		<p>The Data Privacy Act regulates handling of ‘personal information’ and defines this to include ‘information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual’. This can be interpreted to incorporate any footage from visual surveillance equipment.</p> <p>Overt monitoring of access to IT and other equipment</p> <p>In practice, monitoring of IT equipment is undertaken in the Philippines, although its use is restricted under Article III of the Bill of Rights, Section III of the Constitution, which states ‘the privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law’. Additionally, ‘any evidence obtained in violation of this or the preceding section shall be inadmissible of any purpose in any proceeding.’</p> <p>The E-Commerce Act however imposes a duty of confidentiality on individuals.</p>

		<p>Covert monitoring of access to IT and other equipment</p> <p>See above.</p> <p>Reporting hotlines (anonymous)</p> <p>No specific legal restrictions apply to this security measure. In practice however reporting hotlines are not regularly used by local employers.</p> <p>Reporting hotlines (confidential)</p> <p>No specific legal restrictions apply to this security measure. In practice however reporting hotlines are not regularly used by local employers.</p> <p>Use of alerts/automated warning systems to identify unusual employee behaviour (out-of-hours activities, duplicate payments)</p> <p>No specific legal restrictions apply to such security measures.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>Monitoring of communications does take place in the Philippines, but employers should be aware of the provisions of the Anti-Wiretapping Act.</p> <p>In addition, the recent Data Privacy Act regulates handling of ‘personal information’ and defines this to include ‘information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual’. This can be interpreted to cover any recording from audio surveillance equipment.</p>
<p>4.8</p>	<p>Formal investigations</p>	<p>Is there a licensing regime covering investigators?</p> <p>There is no formal legislation in the Philippines covering investigators.</p> <p>Physical surveillance (overt or covert)</p> <p>The extent to which an employer may undertake physical surveillance depends on the risk that such surveillance might intrude on the privacy of an individual, which is protected under the Constitution and the Data Privacy Act. Legal advice should be sought in specific circumstances.</p> <p>Electronic surveillance (e.g. tracking devices)</p> <p>As above. Also, use of such surveillance might infringe the Anti-Wiretapping Act and the Data Privacy Act. Legal advice should be sought in specific circumstances.</p> <p>Visual and communication surveillance (using cameras, video or CCTV)</p> <p>This type of measure is more commonly implemented by large companies and banks.</p>

Communication intercept (including oral, written and electronic communication including bugging devices)

The Anti-Wiretapping Act prohibits and penalises wiretapping and other related violations of privacy of communication. For further details see www.lawphil.net.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

Retrieval of information from computers or databases is permissible, taking into account an individual's right to privacy under the Constitution.

Formal interviews of staff

Formal interviews are commonly undertaken in the Philippines and employees are generally expected to cooperate with such investigations.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

Transactional surveillance is generally permissible although due care should be exercised not to violate general rights to privacy set down in the Constitution.

Search and seizure of evidence, whether electronic or physical (overt or covert)

A search warrant should be secured from the appropriate court prior to the search and seizure of evidence, whether physical or electronic (either overtly or covertly).

Is it either usual or necessary to involve the police in investigations?

It is not necessary to involve the police in investigations. Matters regarding employment are usually handled internally and normally resolved by the employer and the employee. However for criminal matters it is important to involve the police authorities.

If the police are involved, at what stage in the investigation does this generally occur?

The police may or may not be involved in an investigation. The decision as to when and if to involve the police may depend on a number of factors such as the severity of the matter and the speed of response required (the police might not have sufficient resources).

Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?

In the Philippines the police may have limited resources and therefore cannot realistically investigate all cases in detail. An organisation may undertake its own investigation, alone or in conjunction with a third party.

		<p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>The Anti-Money Laundering Act imposes obligations on an employer or individual to report suspicious activity. An employer is not legally obliged to report security incidents to the police if handled internally, although it would have a moral obligation to report matters of national security to the law enforcement authorities.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

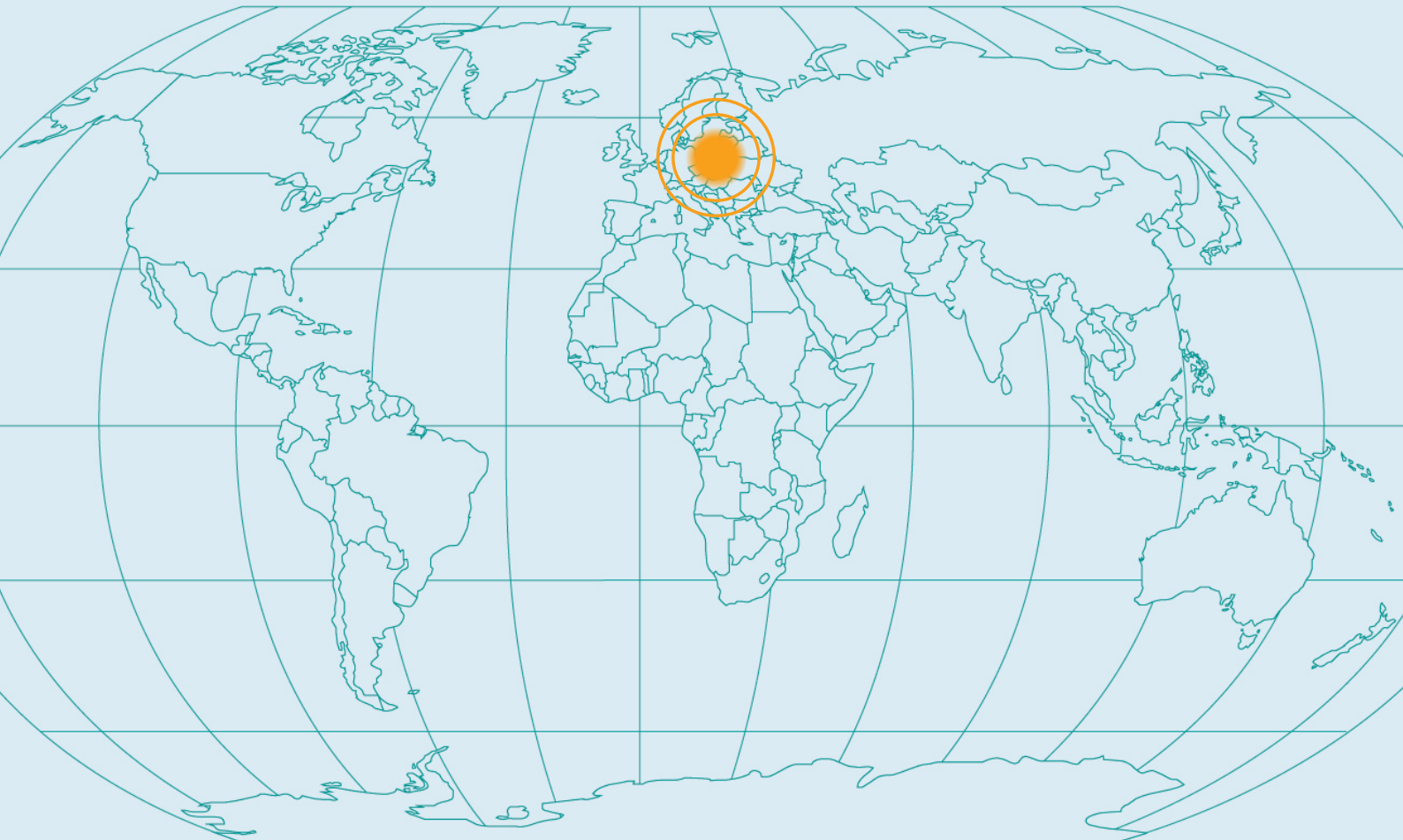
CPNI

Centre for the Protection
of National Infrastructure

SECURITY **WATCHDOG**
Part of Capita plc

Poland

Personnel Security in Offshore Centres



Poland

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1	Introduction	<p>Poland's attraction as an offshore centre is based on a number of factors, most notably its proximity to Western European markets (both geographical proximity and a cultural understanding); language skills, in particular in German; and an established IT services industry. As a member of the European Union (EU), Poland also benefits from consistent laws and regulations that apply elsewhere in Europe. However, a large number of skilled individuals have migrated to other Western European countries in search of opportunities and higher wages.</p> <p>An employer's right to conduct pre-employment security screening in Poland is set out under the Labour Code, which imposes duties on a prospective employee to provide information to an employer. In practice, such information is generally obtained from an employee on commencement of the employment contract, and not before.</p> <p>Using the Personal Data Protection Act, an employer is generally able to apply a range of employee security measures during employment or as part of an investigation.</p>
2 Personnel security measures during recruitment		
2.1	Culture of screening	<p>The Labour Code Act 1974 and the Decree of the Ministry of Labour and Social Policy 2006 define the information that an employer may request from a prospective employee as part of the pre-employment security screening process. Such a process requires the formal consent of the prospective employee under the Personal Data Protection Act 1997 (amended 2006).</p> <p>An employer has a right during the recruitment process to verify documentation relating to the following personal data: name and surname, parents' names, date of birth, place of residence (correspondence address), educational background, previous work history, citizenship and professional qualifications required for the position offered. Additional personal data may be requested if permitted under specific regulations (i.e. for licensed professionals). The candidate must provide his or her consent to gathering such data.</p> <p>If the prospective employee is to have access to confidential, restricted, secret or top-secret data, he or she may be subject to additional levels of security screening.</p>
2.2	Major laws and regulations applying to pre-employment screening	<p>In Poland, the principal legislation governing employee security screening is as follows:</p> <ul style="list-style-type: none"> • the Labour Code Act defines an employee's rights in respect of unfair dismissal; the Code forbids any discrimination in employment relationships, particularly on grounds of sex, age, disability, political views, religious beliefs or trade union membership; and builds on an individual's rights under the Constitution of the Republic of Poland of 1997, which guarantees the equal rights of men and women • Section 10 of the Labour Code also refers to an employer's responsibility to ensure a safe working environment

		<ul style="list-style-type: none"> • Article 22 of the Labour Code prohibits an employer from obtaining criminal records data about a prospective employee unless the provisions of separate laws impose such an obligation • the Employment Promotion and Labour Market Institutions Act of 20 April 2004 governs the issue of work permits and sets out situations in a work permit is not required • the Personal Data Protection Act of 29 August 1997 (amended 2006), is based on the EU Data Protection Directive (95/46/EU). The Act regulates the way in which personal data (including that collected in the course of an investigation on behalf of an employer) can be gathered, retained, stored and destroyed. It allows personal data obtained during an investigation to be retained for as long as is necessary for the duration of the purposes they are used for. The organisation must be able to justify, by reference to the nature of the incident or suspicion or the likelihood of appeal, why continued retention of the data is necessary. An organisation may keep personal data only after getting the approval of the individual concerned. The law sets out civil and criminal sanctions for violations of the Act and is enforced in Poland by the Inspector General for the Protection of Personal Data.
3	Pre-employment checks	
3.1	Identity check	<p>An employer may obtain information concerning a prospective employee's name, address and date of birth (under the Labour Code). An employer may request further identification information, but an employee is not obliged to provide it.</p> <p>In Poland, each adult citizen holds a national ID card (dowod osobisty), so this is available to confirm identification. A passport is also a commonly accepted form of identification.</p>
3.2	Checks on eligibility to work	<p>Polish nationals and members of the EU/EEA do not require work permits in order to work in Poland. Their nationality is generally established on the first day of employment.</p> <p>The prospective employer is responsible for contacting the Polish authorities and obtaining work permit documentation for non-Polish employees. This documentation will be received by the employer once a written employment contract for the employee is provided to the authorities. The work permit fee is from PLN 50 to 200 (valid in February 2014).</p> <p>The issue of work permits, and the categories of employees requiring or not requiring a work permit, are governed by Chapter 16 of the Act on Employment Promotion and Labour Market Institutions.</p>

3.3	Residency checks	<p>Under the Labour Code, an employer has a right to request address information for a prospective employee. Accordingly, it is common practice to undertake residency checks in Poland. Normally this information is verified by the employer on the first day of employment.</p> <p>Address information is provided on the national ID card. Under Article 40 of the Act on Population Register and ID cards of 10 April 1974 there is a legal obligation on individuals to update their residency data if this changes. In practice, individuals often do not update the residency information on the ID card and the enforcement of penalties for non-compliance is not strict.</p>
3.4	Criminal record checks	<p>Name of certificate</p> <p>Information about a person extracted from the National Criminal Register (Informacja o osobie z Krajowego Rejestru Karnego).</p> <p>Department that holds records</p> <p>The Information Office of the National Criminal Register (Biuro Informacyjne Krajowego Rejestru Karnego).</p> <p>Where to apply within country</p> <p>Biuro Informacyjne Krajowego Rejestru Karnego, ul. Czerniakowska 100, 00 – 454 Warszawa, Poland.</p> <p>Telephone: +48 (0) 22 39 76 200 Fax: +48 (0) 22 39 76 205 Email: b-krk@ms.gov.pl Website: http://bip.ms.gov.pl/pl/ministerstwo/struktura-organizacyjna/biuro-informacyjne-krajowego-rejestru-karnego/</p> <p>Information Points for the National Criminal Register can be found at http://bip.ms.gov.pl/Data/Files/_public/bip/krk/wykaz_punktow_informacyjnych_krk.pdf.</p> <p>How to apply within country</p> <p>The application form is available from all Information Points or from http://bip.ms.gov.pl/pl/rejstry-i-ewidencje/krajowy-rejestr-karny/. The form must be submitted at one of the Information Points or sent by post with the proof of payment.</p> <p>The applicant must provide an ID document.</p> <p>Who can apply</p> <ul style="list-style-type: none"> • Individuals • an employer can apply on behalf of an individual only if its right to apply arises from national law • a third party can apply on behalf of an individual only if it has power of attorney and • the information may be requested by a parent or guardian for individuals under 18.

		<p>Cost</p> <p>The cost is PPLN 50.</p> <p>Payment can be made in the National Criminal Register Office or by purchasing a revenue stamp worth PLN 50 and attaching it to the application form.</p> <p>Turnaround</p> <p>The turnaround time is seven days.</p> <p>There is no fast-track service available.</p> <p>Relevant legislation</p> <ul style="list-style-type: none"> • The National Criminal Register Act (24 May 2000) • Ustawa o Krajowym Rejestrze Karnym Dz.U.2012 poz.654 • the Penal Code – Chapter 12 (6 June 1997) • Kodeks karny Dz.U.1997.88.553 • the Personal Data Protection Act (29 August 1997) • Ustawa o ochronie danych osobowych. Dz.U. 2002 nr 101 poz. 926 and • Article 106 of the Polish Criminal Code. <p>Further information can be obtained from the CPNI guidance on <i>Overseas Criminal Record Checks</i> which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>
3.5	Education checks	<p>The employer may ask for a university or school certificate, or recommendations from the institution, and has a right to do so under the Labour Code.</p> <p>An employer would typically check education certificates on the first day of employment or thereafter. Checks will be made directly with the educational establishments concerned, to verify that data provided by the employee is accurate and complete.</p>
3.6	Qualification checks	<p>An employer may carry out qualification checks. The process is similar to that for education checks (see Section 3.5).</p>
3.7	Employment references	<p>An employer may check employment references. This will be undertaken directly with previous employers and requires the consent of the individual concerned.</p> <p>Where an individual provides a letter of reference to a prospective employer during the recruitment process and a name and contact details are given for the reference provider, the employer may approach the provider of the reference for further information.</p> <p>Character references may be taken up with persons of standing in the community (such as a police officer or a professional) where such individuals are nominated by the prospective employee. There is no legal obligation on the referee to provide any information requested.</p>

3.8	Financial/ credit checks	Although there is no legal provision for the performance of financial or credit checks in Poland, there is no infrastructure in place for undertaking such checks and in practice they are not regularly performed.
3.9	Substance abuse screening	Although there is no legal provision for these checks, there is no infrastructure in place for undertaking them and in practice they are not regularly performed.
3.10	Occupational health checks	An employer may only request that such a check is undertaken after an offer of employment has been made. The employee can start working after any occupational health check has been successfully completed. Such checks are generally undertaken at a clinic designated by the employer. Retention of data must comply with the Personal Data Protection Act.
4	Personnel security measures during employment	
4.1	Legal requirements	The main laws and regulations that apply to security measures during employment are as follows: <ul style="list-style-type: none"> • the Labour Act of 26 June 1974 • the Personal Data Protection Act of 29 August 1997 (amended 2006). • the Confidential Data Protection Act (the legislation is available only in Polish) • the Act on Services of Private Detectives (the legislation is available only in Polish) and • the Trade Unions Act (the legislation is available only in Polish). <p>Trade union membership in Poland is relatively low and has continuously declined since the 1990s. The two largest trade union confederations are NSZZ Solidarnosc and OPZZ.</p> <p>Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 established a general framework for informing and consulting employees in the European Community and was enforced in Poland through the Act of 7 April 2006 on informing and consulting employees. Under this Act all employers who employ more than 50 individuals must allow an employees' representative to be elected. The representative is not entitled to consult on the termination of labour agreements, which right is confined to trade unions and their members.</p>
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	The Labour Act defines the rights and duties of both employers and employees. It defines the circumstances in which an employer may take formal action against an employee who breaks any laws or regulations and governs other forms of conflict between the employer and employee. The Act lays down penalties and sanctions for both the employee and the employer.

4.4	Local legislation that specifically governs the rights of the employee	The Labour Act is the primary legislation governing the rights of the employee in the workplace.
4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	Under the Labour Act an employee may bring a complaint to the National Labour Inspectorate (PNLI) or to the Labour Court. The National Labour Inspection Office may carry out a compliance audit and can levy fines against employers for non-compliance. Employees can report employers anonymously to the Office.
4.6	What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?	<p>An employee's rights are protected under the Labour Code. An employee seeking to challenge his or her dismissal would generally bring a claim to a Labour Court. In Poland the process for dismissal of employees is complex and increasingly regulated by the courts. Where the employee is a member of a trade union, the union must be involved in the dismissal process. As labour law in Poland is increasingly complex, legal advice should be sought in specific circumstances.</p> <p>The disciplinary process is defined under the Labour Code, Article 52. Before an employer may terminate the employment of an employee on disciplinary grounds, it must meet the following formal requirements:</p> <ul style="list-style-type: none"> • the dismissal should be executed in writing • the document should clearly state the reason for termination to the employee, which should be actual and justified • the employer must communicate to the employee their rights to challenge the termination at a Labour Court and name the competent court and • if the employee is a trade union member, the employer must consult the trade union. <p>Under Chapter 5, Article 52 of the Labour Code, an employer may terminate the employment contract of an employee without notice for serious violations of employee duties, such as criminal behaviour or as a result of actions by the employee that render him or her ineligible to perform his or her duties.</p>

4.7

**Availability
of security
measures**

Restriction of access to premises

For organisations with more than 20 employees, work regulations stipulate that an employer must maintain a register of employees' entry and exit times. This is usually performed by using access cards or registration in a book. Organisations with fewer than 20 staff may incorporate such measures into their work regulations, at their discretion. There are no other specific legal restrictions on controlling access to premises, although the storage and dissemination of biometric data (if used) is subject to the provisions of the Personal Data Protection Act.

Restriction of access to certain rooms/zones on the premises

Access restrictions are generally defined in the employer's procedures in such a way as to prevent unauthorised individuals from accessing restricted areas. Where confidential, restricted, secret or top-secret data are held, such data must be secured in accordance with Chapter 9 of the Confidential Data Protection Act.

Physical screening (on entry/exit)

If physical screening measures are used, this should be stated in the employer's regulations or handbook. Employees should be informed that physical searches may occur.

Prohibition of removal of data from the premises (hard-copy)

An employer has a general duty and right to maintain confidential data (in accordance with data protection legislation). The terms of the Confidential Data Protection Act also apply. Three types of data are treated as sensitive under Polish law:

- *commercially secret data* – provisions on access to the data and their removal from the premises should be included in work regulations and employment contracts
- *state secrets and qualified commercial secrets* – the creation of, processing and access to state and qualified commercial secrets is subject to specific restrictions, which include access procedures and controls, and special training for employees to whom access to information is granted; such access is controlled by the ABW (the Internal Security Agency) and
- *personal data* – access must be limited to employees who are specifically authorised by the employer. The Personal Data Protection Act requires internal procedures on security and the processing of personal data to be established.

Penalties for unauthorised release of these types of information may range from disciplinary processes to criminal penalties.

Prohibition of removal of data from the premises (electronic)

See above.

Visual surveillance (CCTV or other cameras), either overt or covert

Use of visual surveillance measures is generally subject to data protection legislation; use should not intrude on personal privacy and should be in proportion to the risks faced. It is good practice for an employer to clearly state in the employer's regulations or handbook that such security measures are in use, and to inform employees in advance of their use. Such measures should only apply to the employer's place of work and its equipment. In Poland the use of visual surveillance measures is increasingly widespread.

Overt monitoring of access to IT and other equipment

See above.

Covert monitoring of access to IT and other equipment

See above.

Reporting hotlines (anonymous)

It is good practice to set out the policy for the use of reporting hotlines in the employer's regulations or handbook. In practice, few employers in Poland use reporting hotlines.

Reporting hotlines (confidential)

See above.

Use of alerts/automated warning systems to identify unusual employee behaviour (out-of-hours activities, duplicate payments)

The use of alerts or automated warning systems does not generally infringe data protection legislation. As a matter of good practice, the use of such a security measure should be set out in the employee regulations or handbook.

Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)

See above. In particular, monitoring of personal calls or other communications may breach personal privacy under data protection legislation.

4.8

Formal investigations

Is there a licensing regime covering investigators?

Private detectives are required to apply for a licence and to hold civil liability insurance.

The activities of private investigators are governed by the Act on Services of Private Detectives of 6 July 2001.

Physical surveillance (overt or covert)

Physical surveillance must comply with data protection legislation. Its use should be set out in the employer's regulations or handbook.

Other than the police, only licensed private detectives may undertake physical surveillance activities, and a written agreement should be signed by the detective and the employer requesting surveillance. The Act on Services of Private Detectives states that private detective services can be used, amongst other purposes, to investigate relationships between individuals, commercial relationships and cases subject to formal criminal investigations.

Electronic surveillance (e.g. tracking devices)

See above.

Visual and communication surveillance (using cameras, video or CCTV)

The use of visual surveillance measures may be acceptable where the employee is informed in advance of their use and the surveillance relates solely to office premises or equipment owned and controlled by the employer. Employees are generally notified of the use of such measures through the work regulations or employment contract.

Communication intercept (including oral, written and electronic communication including bugging devices)

See above.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

See 'Visual surveillance' above. Such surveillance may only extend to equipment owned and controlled by the employer (for example, business computers, mailboxes, credit cards etc). In Poland there is an increasing trend towards the use of such security measures.

Formal interviews of staff

Interviews of staff are subject to Constitutional and human rights safeguards. Where the interview is undertaken as part of a criminal investigation, the police/law enforcement authorities must be involved, or the information gathered may not be admissible in court.

In practice, formal interviews take place frequently as part of formal investigations (although an employee is not obliged to answer questions).

		<p>Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, computer access logs and financial transactional data)</p> <p>See ‘Visual surveillance’ above. An employer may conduct such surveillance provided this pertains to its own equipment, systems or property (such as telephones or credit cards). In Poland there is an increasing trend towards the use of such security measures.</p> <p>Search and seizure of evidence, whether electronic or physical (overt or covert)</p> <p>The Personal Data Protection Act applies to the use of search and seizure in Poland, and protects personal data and documents. There is an increasing use of measures to secure electronic evidence, for example by taking images of computer hard drives.</p> <p>Is it either usual or necessary to involve the police in investigations?</p> <p>For non-public sector employers, the employer may choose to involve the police. Public sector employers are required to involve the police from the initial suspicion stage.</p> <p>If the police are involved, at what stage in the investigation does this generally occur?</p> <p>Police involvement must occur at an early stage in cases where public sector employers are involved. Typically, police involvement is later for non-public sector employers or in cases where there is a criminal aspect to the investigation.</p> <p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>In practice, the police are not frequently involved in formal internal investigations, for a variety of reasons. Most notably, employers do not wish to lose control over the direction of an investigation and the presence of the police can cause significant disruption to the business.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>For non-public sector employers, the employer may choose to involve the police. Public sector employers are required to involve the police from the initial suspicion stage.</p> <p>Other legal considerations not covered above.</p> <p>Various authorities including the police, the Central Anticorruption Office (CBA), the Tax Office and the Customs Office are allowed to initiate investigations of their own volition, and to seize and secure evidence, including the employer’s documents.</p> <p>Under the Anti-Money Laundering Regulations, banks and financial institutions, tax advisors, lawyers (and certain other categories of employer defined by the Act) are obliged to monitor and report suspicions of money laundering.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

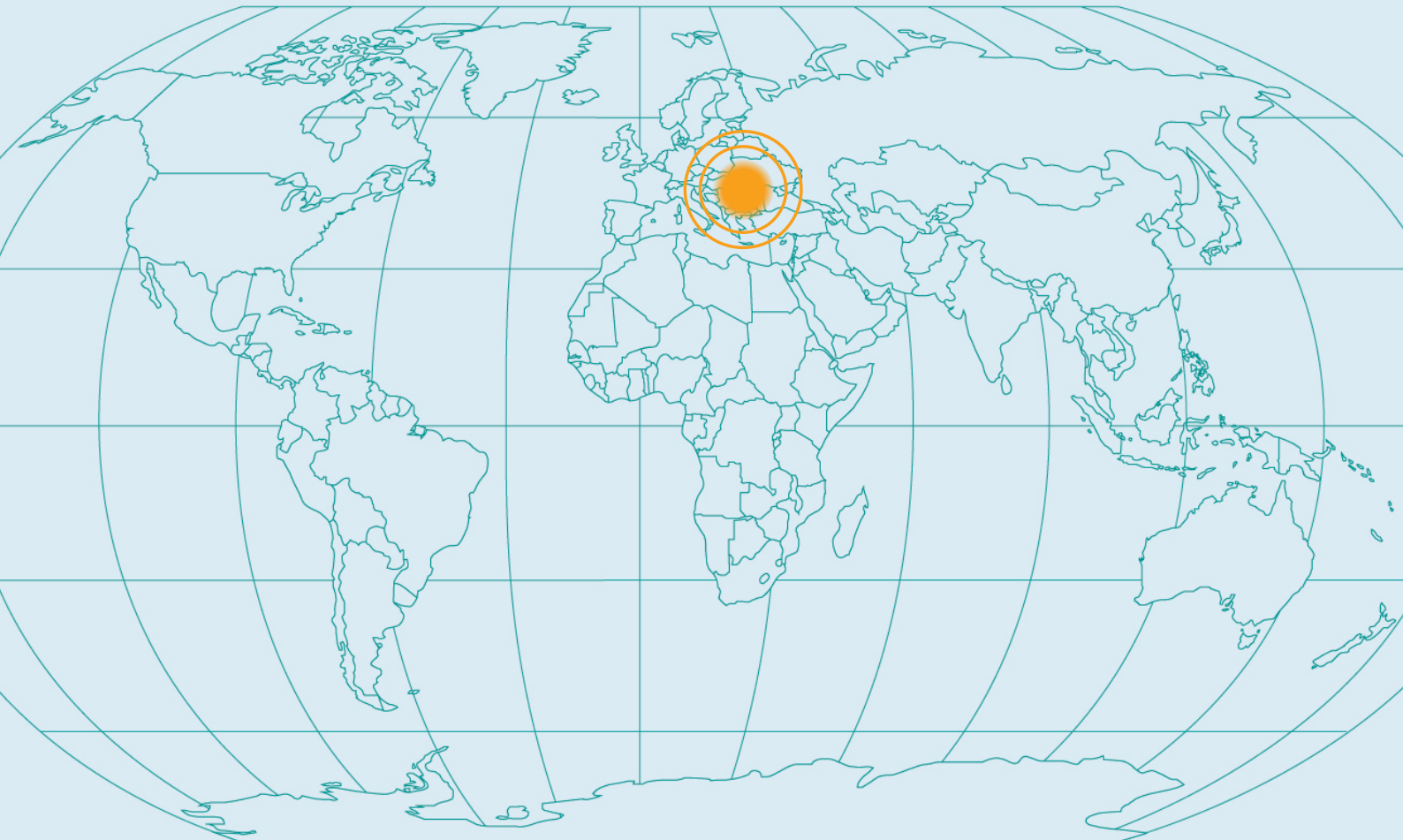
CPNI

Centre for the Protection
of National Infrastructure

SECURITY WATCHDOG
Part of Capita plc

Romania

Personnel Security in Offshore Centres



Romania

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1	Introduction	<p>Romania is a common outsourcing location in Central and Eastern Europe, in particular for IT outsourcing and business process outsourcing (BPO) (although the country has less IT specialisation than India). Romania has a shorter history of providing such services than other major centres such as India.</p> <p>Romania benefits from available language skills, in particular French, and from a knowledge of the culture and customs of European firms.</p> <p>As a member country of the European Union (EU), Romania has enacted a range of regulations to bring it into line with other European countries. Accordingly, it has data protection legislation that protects the rights of both employee and employer as well as an established labour code.</p> <p>In Romania an employer’s ability to conduct investigations into criminal matters is limited, as the police must be involved in the evidence-gathering process for this to be admissible in a court of law.</p>
2 Personnel security measures during recruitment		
2.1	Culture of screening	<p>Most subsidiaries of foreign companies in Romania use pre-employment screening procedures as part of their recruitment process. In many cases, use of pre-employment security screening is determined by a company’s group policy. The screening process is generally undertaken by the prospective employer’s Human Resources department.</p> <p>It is common practice for a higher level of screening to be applied to more senior staff or staff with access to more sensitive information.</p> <p>Pre-employment screening processes vary between organisations. Most organisations verify academic qualifications, health status and previous employment references as a minimum. For all employees, the Romanian Labour Code requires only that all employees should provide a medical certificate that proves that they are physically able to perform their duties (see Romanian Labour Code, Article 27).</p>
2.2	Major laws and regulations applying to pre-employment screening	<p>The main laws and regulations that apply to pre-employment screening procedures in Romania are as follows:</p> <ul style="list-style-type: none"> • the Romanian Labour Code (Law No. 53/2003, as amended 2010), the relevant articles of which include: <ul style="list-style-type: none"> – Article 3: the fundamental right to work and freedom to choose a profession – Article 4: prohibition of forced labour – Article 5: equal treatment for all employees; discrimination prohibited under this Article includes that based on: <ul style="list-style-type: none"> • gender • sexual orientation • genetic characteristics • age • race

- nationality
- skin colour
- ethnicity
- religion
- social origin
- disability
- marital status and
- union activity and membership
- Article 29: verification of skills
- Article 39: main rights and obligations of the employee and
- Article 40: main rights and obligations of the employer.

There are two laws governing personal data protection:

- **Law No. 506/2004 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector** (replacing Law 676/2001) which closely follows the EU Directive on personal data processing and privacy protection in the electronic communications sector (**2002/58/EC**). and
- **Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data** implements the EU Data Protection Directive (1995/46/EC).

Enforcement of the laws on data privacy is supervised by the Personal Information Supervisory Agency. It has the role of controlling the legitimate collection and use of personal data. It maintains records on all personal data operators and the operations they perform regarding personal data. The agency also handles complaints from individuals and can authorise, suspend or terminate the activities of personal data operators. In addition to the Personal Information Supervisory Agency two national bodies regulate electronic communications:

- The **National Authority for Management and Regulation in Communications** (ANCOM) is the supervisory body for all communications operators (telephone service providers, internet service providers, cable or satellite TV providers, etc). Its responsibility is to issue and enforce all specific regulations for these operators, in order to protect all personal data collected by the operators and to protect the security and confidentiality of electronic communication; and
- The **People's Advocate Office** (also referred to as the Ombudsman). Law no. 35/1997 on the organisation and functioning of the People's Advocate was amended to create a Private Information Protection Office (PIPO), which is specifically involved in protecting the rights of individuals to privacy in relation to electronic communication data. It has the authority to appoint inspectors who control the implementation of the law by electronic communication operators. It can issue fines for irregularities found during inspections.

3	Pre-employment checks	
3.1	Identity check	<p>In Romania it is common to check an individual's identity (given name, date of birth, parent's names and addresses). This check is usually done when the work contract is concluded between the parties.</p> <p>The Romanian National Identity Card (<i>Carte de identitate</i>) is the main document used in Romania to certify a person's identity. The ID card has several verification features in the positioning of the graphic and text elements on the card and correlations between data within the document.</p> <p>If a person does not have all the documents necessary for an ID Card to be issued or is a Romanian citizen with a permanent residence abroad but living temporarily in Romania, a temporary ID (<i>Carte de identitate provizorie</i>) can be issued for a maximum period of one year.</p> <p>A passport or driving licence is also an acceptable identity document.</p>
3.2	Checks on eligibility to work	<p>This does not apply to Romanian nationals nor to EU citizens who have an unrestricted right to work in Romania.</p> <p>Work permits for foreign nationals are issued directly to the employer by the Romanian General Inspectorate for Immigration. Only after a work visa has been issued can the employee apply for a work permit. The work visa grants permission to enter the country and to obtain a work permit. The work visa is valid for only 90 days and is issued by the Romanian Customs Service. The work permit is a document issued by the Labour Migration Office that allows a foreigner to be employed and to reside in the country for the duration of employment.</p> <p>Government Expeditious Ordinance 194/2002, Article 44 considers a 'foreign citizen' to be any person who is not a national of an EU or EEA country.</p> <p>Further information is available from the Romanian Interior Ministry (MAI) at www.ori.mai.gov.ro/detalii/pagina/en/Admisie/62.</p>
3.3	Residency checks	<p>Residency information is included on the ID Card.</p> <p>The Card carries the registered address of the prospective employee. Although, under Government Expeditious Ordinance 97/2005, Article 18, a person is required to obtain a new ID Card within 15 days of changing address, often individuals do not do so because of the bureaucracy involved and the relatively small fine (between €10 and €20).</p>
3.4	Criminal record checks	<p>Name of certificate</p> <p>Criminal Records Certificate (<i>Certificat de Cazier Judiciar</i>).</p> <p>Department that holds records</p> <p>The Directorate of Criminal Records, Statistics and Operational Registers within The General Inspectorate of Romanian Police.</p>

Where to apply within country

A list of county police stations at which applications can be made for criminal record certificates can be found at www.politiaromana.ro/site_judetean.htm.

The national office is:

The Directorate of Criminal Records, Statistics and Operational Registers,

The General Inspectorate of Romanian Police,
13–15 Stefan cel mare Street,
2 District,
Bucharest,
Romania.

Telephone: + 40 (0) 21 208 25 25

Fax: + 40 (0) 21 317 87 90

Email: cazier@politiaromana.ro or cazier.eu@politiaromana.ro

Website: www.politiaromana.ro/directia_cazier.htm

How to apply within country

Applications can be submitted to any police station along with:

- the applicant's ID card
- a fiscal stamp with a value of LEI 2
- a receipt for the payment of tax of LEI 10 and
- a completed, hard-copy application form.

Who can apply

Individuals; however, if a Romanian person is born abroad and does not have an address in Romania, they can apply for a Romanian criminal records certificate only through a representative.

A representative can apply if it has a documented power of attorney, which needs to be validated by a public notary, Romanian diplomatic mission or consular office. Employers cannot apply directly to obtain an individual's criminal record.

Cost

LEI 2 for a 'fiscal stamp', which can be purchased at all post offices; and LEI 10 for the accompanying tax, which can be paid at the Financial Administration.

Turnaround

Turnaround time from when the request is submitted in Romania is between three and ten working days.

Legislation

Law No 290, 24 June 2004, governs the disclosure of criminal records in Romania.

Further information can be obtained from the CPNI guidance on Overseas Criminal Record Checks which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/

3.5	Education checks	<p>An employer may require a prospective employee to provide evidence of their level of education. Information confirmed may include the educational establishment attended and level of education level achieved by the individual. For individuals operating in the health services and other specific professions (pilots, welders, miners, drivers etc.) this is common practice, owing to the risk involved.</p> <p>Character evaluations are usually not available because of the class sizes in Romanian schools and universities. Confirmation may be sought directly from the educational establishment(s) concerned.</p> <p>The existence and accreditation of the educational institution can be verified using the Ministry of Education website: www.edu.ro.</p> <p>In industries where it is not mandatory to obtain a particular certification/qualification, employers often use tests and interviews, together with a testing period clause in the contract (for higher-risk positions), during which the knowledge of the employee is assessed.</p> <p>Law 677/2001 on the processing of personal data prohibits the collection and storage of personal information without consent. However, even if an employee does consent to the employer gathering such information, the employer must notify its intentions to the National Personal Supervision Agency at least 30 days before collecting such data. The Agency can prohibit the employer from collecting or using such information, even if written consent has been obtained from the prospective employee.</p>
3.6	Qualification checks	<p>A number of organisations maintain records of practitioners and individuals qualified in that profession. These include:</p> <ul style="list-style-type: none"> • architects • certified accountants • certified auditors • valuers • lawyers • bailiffs and process servers – technical experts • pharmacists • insolvency practitioners • dental practitioners • veterinarians • notaries public • nurses and • geologists. <p>Character evaluations are usually not available.</p> <p>Information regarding political or religious convictions, sexual orientation, ethnicity or social origin cannot be obtained.</p> <p>To verify the membership of a professional association most organisations provide a search function on their websites. This link provides access to a website on which professional membership can be verified for a number of institutions: http://www.uplr.ro/eng/principale.html</p>

3.7	Employment references	<p>It is normal practice for employers in Romania to provide references for former employees. This includes basic information such as dates of employment and position(s) held.</p> <p>The Labour Code requires only basic employment information to be confirmed and former employers do not usually provide references covering the performance of the employee. The request should be directed to the respective former employer(s). The consent of the individual is generally required before former employer(s) will disclose information. This is governed under the Romanian Labour Code, Article 29; see http://www.codulmuncii.ro/en.</p> <p>Information regarding political or religious convictions, sexual orientation, ethnicity or social origin can be neither requested nor provided.</p> <p>Obtaining character references from previous employers is not particularly widespread or common. If it is undertaken, typically a reference would be sought from a previous line manager.</p> <p>It is not established practice in Romania to request character references from persons of standing in the community (for example, lawyers, policemen, judges, etc).</p>
3.8	Financial/ credit checks	<p>There are no established commercial credit bureaux in Romania that provide credit verification suitable for use as part of pre-employment security screening.</p> <p>The only organisation that maintains this type of information for individuals is the Biroul de Credit (Credit Bureau), but the information is available only to registered members. The Bureau only accepts applications from banks, insurance companies and leasing companies.</p>
3.9	Substance abuse screening	<p>Substance screening is not yet an established practice in Romania and the availability of such tests is very limited. They are performed in high-risk professions (health services, pilots, etc).</p> <p>Explicit consent by the individual would be required. In practice, an employee would normally attend a medical centre (generally one approved by the employer) and provide a sample (blood, urine). The results of the test are transmitted back to the employer.</p>

3.10	Occupational health checks	<p>Occupational health checks are a requirement under the Romanian Labour Code: ‘A person may only be employed on the basis of a medical certificate, attesting that the concerned person is able to perform the respective activity’.</p> <p>In practice, a medical test is tailored to the proposed role of the employee. The test will always include a fitness test (general health check-up), an eyesight test and blood will be tested for transmissible diseases. The ability of disabled persons to undertake a given role will be assessed against the prospective position. For example, an employer would not be able to hire a construction worker with movement coordination problems, but that person might be employed in an administrative or office role. The medical test is designed to minimise the health risks for both the employer and the employee.</p> <p>An occupational health check cannot include tests to determine whether a prospective employee is pregnant.</p> <p>This is covered under the Romanian Labour Code, Article 27.</p> <p>Occupational health checks are generally undertaken at a health centre approved by the employer.</p>
4	Personnel security measures during employment	
4.1	Legal requirements	<p>In Romania the major legal requirements relating to ongoing personnel security measures are as follows:</p> <ul style="list-style-type: none"> • The Romanian Constitution, adopted in 1991, recognises rights to privacy, the inviolability of the home, freedom of conscience and of expression. In practice, although the rights and freedoms of individuals are guaranteed under the Constitution, an employee bringing a grievance in a work-related situation is more likely to seek redress through labour legislation (see below) which is more explicit. • The Romanian Labour Code (see above). Within the Code, the National Collective Labour Agreement sets out the main rights and obligations of both employees and employers and also regulates the relationship between employees, trade unions and employers. Industry Labour Agreements are concluded between trade unions and employers in specific industries and usually contain clauses that are advantageous for employees. The National Collective Labour Agreement includes the minimum clauses and conditions to be included in any individual labour agreement. The Romanian Labour Code is generally perceived to favour the interests of the employee. In some cases, the Labour Code is not consistent with subsequent labour legislation (in such cases the law favouring the interests of the employee would prevail).

		<ul style="list-style-type: none"> • Law No. 677/2001 regarding the protection of personal information (see Section 2.2). • Law No. 506/2004 regarding the protection of personal information within electronic communication systems (see Section 2.2). • The Romanian Penal Code and Penal Procedure Code define criminal activities, the sanctions for these acts and the procedures to be followed in prosecuting such a case at court. They include guidance on information that is considered admissible in court. <p>Trade unions exist at a national level in Romania, and also at an employer level. For a union to be legally established it requires at least 15 members in the same profession or industry, even though the members might work for different employers. If the employer has more than 20 employees, the employees can designate representatives to negotiate with the employer. Trade union activity in Romania is governed under Law No. 54/2003.</p>
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	<p>The National Collective Labour Agreement, which covered all Romanian workers and was fundamental to establishing minimum terms and conditions, was abolished by the Social Dialogue Act passed in 2011.</p> <p>The 2011 Act includes more protective measures for trade unions and simplifies the process for initiating industrial action, but has been criticised for limiting the availability of collective bargaining.</p> <p>The following rights and obligations are minimum requirements in Romania under the Labour Code.</p> <p>Rights of the employer</p> <ul style="list-style-type: none"> • The right to organise and manage the entity • the right to define objectives and responsibilities for the employee, within the terms of the labour law • the right to issue mandatory regulations for employees, as long as these regulations comply with the law • the right to control the performance of tasks assigned and • the right to record disciplinary offences and to sanction these offences according to the law, to internal procedures and the applicable work contract. <p>Obligations of the employer</p> <ul style="list-style-type: none"> • To inform the employees about work conditions and work-related elements • to provide permanent technical and organisational conditions, set out in work standards, and an appropriate work environment • to inform the employees periodically about the financial position and performance of the entity, although it may withhold secret or sensitive information that could cause damage if communicated outside the entity

- to consult with trade unions or employee representatives over decisions that could significantly affect the employees' rights and interests
- to pay all contributions and taxes owed by the entity, and also to collect and transfer all contributions owed by its employees
- to implement and operate a General Register of Employees
- at an employee's request, to issue all documents needed to prove his/her employment status and
- to ensure the confidentiality of the employees' personal information.

In addition to these obligations, the employer has certain specific obligations that relate to dismissal procedures. In practice these obligations make it difficult for an employer to dismiss an employee.

The main obligations may be summarised as follows:

- if an employee develops a medical condition that makes him or her unable to perform their role, the employer must provide an appropriate alternative job and proper requalification training for it; if the employer cannot provide an alternative job, it must search for one through the local employment agency
- if a female employee requests an additional year of unpaid maternity leave, on top of the two years provided by law, she cannot be dismissed during this period
- if an individual retires for medical reasons and subsequently regains his or her work abilities, he or she must be re-employed in a position as close as possible to the position previously held
- the refusal of an employee to accept a change to the contract of employment does not give the employer the right to cancel the contract
- an employee who has committed a disciplinary offence can be dismissed only after the facts, the circumstances, the degree of guilt, the damage suffered and the general behaviour of the employee have been evaluated by a disciplinary committee, designated by the employer, and dismissal has been proposed by the committee
- an employee can be dismissed for incompetence if an evaluation committee, designated by the employer and including at least one trade union member, reaches this conclusion after comparing the employee's performance with the objectives in his/her job description, and where new technology is introduced, an employee's performance can be assessed only if he/she has received appropriate training in the new technology and
- employees returning from maternity/paternity leave cannot be subject to performance evaluation within six months of their return.

<p>4.4</p>	<p>Local legislation that specifically governs the rights of the employee</p>	<p>Rights of the employee</p> <ul style="list-style-type: none"> • To receive payment for the work done. The level of the statutory minimum wage is established each year by a Government Decision. Decision no. 871/2013 in January 2014 increased the minimum wage to LEI 850 per month for a full-time role (168 hours per month). Employers are bound by this rate and cannot pay below it. A second increase to LEI 900 per month is planned for 1 July 2014. • To daily and weekly rest. Normal working time is 40 hours a week, and restricted to eight hours a day. Overtime is limited to eight hours per week and needs the employee’s consent. • To annual leave. The employee has the right to a minimum 21 days’ paid vacations per year plus 10 days defined as national holidays. Also, the employee has the right to additional days for family events (marriage, birth, funeral) and is entitled to two years’ maternity/ paternity leave. • To equal treatment and opportunities. • To dignity at work. • To security and health protection at work. The employer has to provide all necessary protective equipment and at least once a year a free medical check-up. • Access to professional training. • To information. • To be involved in establishing and improving the conditions of work and the work environment. • To protection against dismissal. • To collective and individual negotiations. • To participate in trade union activities. • To establish or be a member of a trade union. <p>Obligations of an employee</p> <ul style="list-style-type: none"> • To meet the objectives set out in the job description. • To comply with work ethics regulations. • To comply with internal regulations, and collective and individual work contract provisions. • To be loyal to the employer in performing work duties. • To comply with security and health regulations set by the organisation. • To work confidentiality.
<p>4.5</p>	<p>What avenues are open to employees who seek to challenge an employer’s use of security procedures?</p>	<p>Individuals may bring action against their employer under the legislation detailed in Section 4.1. If the employee is a union member, the union may provide assistance to the employee in settling the claim.</p>

4.6	<p>What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?</p>	<p>An employee may bring a civil claim to court. An employer may not seek to dismiss an employee for bringing such an action.</p> <p>Where an employee is subject to disciplinary proceedings the employer must establish an evaluation committee, in which a union member may be a non-voting member. The committee must undertake a disciplinary investigation into the facts of the incident.</p> <p>The employee must be provided with at least five days' notice prior to the committee hearing to establish the facts. The committee will establish the guilt of the employee in relation to the allegations and will issue a sanctioning decision. The decision can be appealed in court.</p>
4.7	<p>Availability of security measures</p>	<p>Restriction of access to premises</p> <p>No specific restrictions apply.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>No specific restrictions apply.</p> <p>Physical screening (on entry/exit)</p> <p>This type of measure is not illegal although it is not common practice in Romania.</p> <p>Prohibition of removal of data from the premises (hard-copy)</p> <p>There is no specific reference to prohibiting the removal of data from premises within Romanian legislation. In practice, an employer in Romania is likely to restrict the dissemination of confidential data through its own policies and procedures, and the employment contract with the individual employee.</p> <p>Prohibition of removal of data from the premises (electronic)</p> <p>See above.</p> <p>Visual surveillance (CCTV or other cameras), either overt or covert</p> <p>Under data protection legislation action taken by an employer should be proportionate to the threat faced. Monitoring of 'private' areas (such as changing rooms or toilets) is therefore unlikely to be allowable. The use of visual surveillance measures is generally publicised if it is part of company policy. If an employer chooses to install covert security systems on the work premises, the results of such surveillance will not be admissible in a court of law, unless such surveillance is undertaken under a court order and in collaboration with police or prosecutors.</p> <p>Overt monitoring of access to IT and other equipment</p> <p>Aside from matters of national security (that are governed by specific legislation) the use of overt monitoring is generally publicised if it is part of company policy.</p>

		<p>Covert monitoring of access to IT and other equipment</p> <p>Companies in Romania commonly maintain logs of access to IT and other equipment (and have a right to do so where this is company property). Employers commonly warn employees that monitoring procedures may be used as a security measure.</p> <p>Reporting hotlines (anonymous)</p> <p>Employers in Romania may make use of reporting hotlines, but in practice their use is limited. Individuals may report concerns over criminal behaviour to the police under conditions of anonymity and individual company policy will generally dictate procedures for reporting from within the employer’s organisation.</p> <p>Reporting hotlines (confidential)</p> <p>See above.</p> <p>Use of alerts/automated warning systems to identify unusual employee behaviour (out-of-hours activities, duplicate payments)</p> <p>No specific laws or regulations apply to the use of automated warning systems; their use is generally publicised if it is part of company policy.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>The use of overt or covert monitoring of communications is covered by Law 506/2004 concerning protection of personal data sent over electronic communications.</p> <p>Monitoring of telephone conversations may only be undertaken on equipment owned and controlled by the employer.</p>
<p>4.8</p>	<p>Formal investigations</p>	<p>An employer’s ability to gather evidence as part of the formal investigation process is strictly limited under the Romanian Penal Code. The Code generally requires that the police are involved in the evidence-gathering process.</p> <p>Is there a licensing regime covering investigators?</p> <p>Private investigators in Romania are regulated by Law No. 329/2003. The law requires private investigators to hold a professional certificate and register with the local police authorities.</p> <p>Physical surveillance (overt or covert)</p> <p>Surveillance of an employee by any means can only produce evidence admissible in court if a mandate is issued by a judge. This applies to video evidence, phone conversations and electronic communications. Most evidence collecting is done by the police and prosecutors for criminal cases.</p>

Electronic surveillance (e.g. tracking devices)

See above.

Visual and communications surveillance (using cameras, video or CCTV)

Although an employer may choose to use visual and communications surveillance to monitor employees' activity, its use as part of an investigation (as evidence) is a matter for the courts. Local practice is for such evidence to be collected only by the police and prosecutors. Evidence collected is subject to the Romanian Penal Code.

Communication intercept (including oral, written and electronic communication including bugging devices)

It is local practice that such evidence may be collected only by a specialised unit of the Romanian Information Services. Evidence collected in this way is subject to the Penal Procedure Code. Data privacy legislation does not specifically apply to criminal investigations.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

See 'Communication intercept' above.

Formal interviews of staff

Employers have the right to interview staff, but for the results of such interviews to be admissible in court, the interviews must be performed by the police or a public prosecutor.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

See above.

Search and seizure of evidence, whether electronic or physical (overt or covert)

See above.

Is it either usual or necessary to involve the police in investigations?

It is not necessary to involve the police in all investigations, but it is usual to involve them in investigating a suspected crime, as usually a court will not accept evidence collected directly by the employer.

If the police are involved, at what stage in the investigation does this generally occur?

The decision as to when and if to involve the police may depend on a number of factors including:

- the severity of the matter
- the credibility of the person making the allegations
- the reputational risk that will materialise if the matter becomes public and
- the substance of the damage caused.

		<p>Police are usually involved in cases of crimes in which the company could be considered liable as a result of its failure to report, or in relation to issues which the company seeks to bring to court.</p> <p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>In Romania the police have limited resources and therefore cannot realistically investigate all cases in detail. An organisation may undertake its own investigation, alone or in conjunction with a third party. However, if the organisation has strong suspicions that a crime has occurred (e.g. fraud, theft, forgery, money laundering) or where an accident occurs in the workplace, it is obliged to report the matter to the police in order for the case to be prosecuted.</p> <p>Usually the organisation will be required to provide the prosecutors with all relevant evidence, including personal data relating to employees who could be considered witnesses or accomplices.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>Under the Romanian Penal Code any suspicions of money laundering, theft, fraud or forgery, or workplace accidents must be reported to the police. In addition, all cash transactions or external money transfers exceeding €15,000 (or equivalent) must be reported to the National Office for Money Laundering Prevention.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

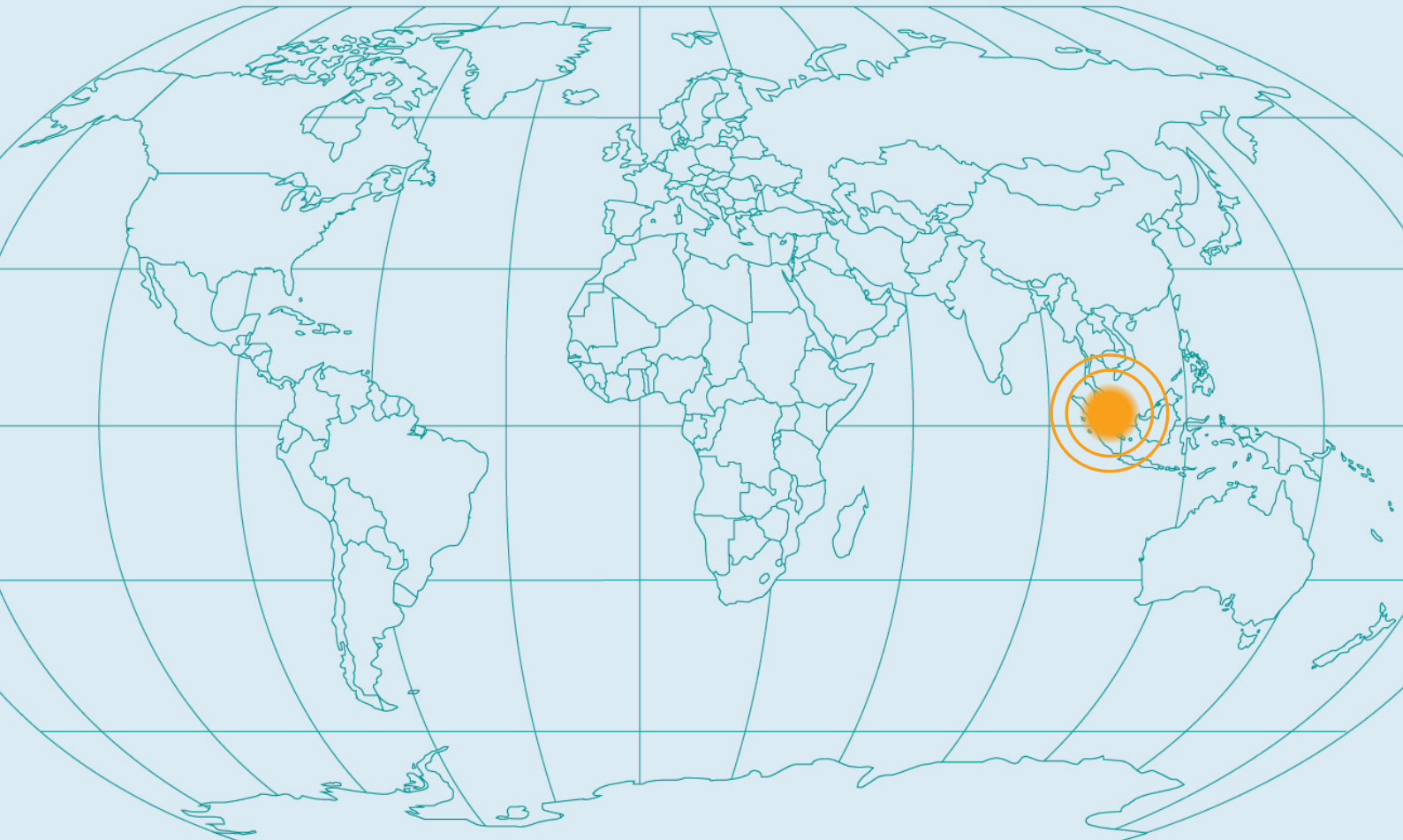
CPNI

Centre for the Protection
of National Infrastructure

SECURITY WATCHDOG
Part of Capita plc

Singapore

Personnel Security in Offshore Centres



Singapore

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1

Introduction

Singapore's history began as an international trading post when the British settled in 1819. Singapore joined the Malaysian Federation in 1963 only to break away two years later to claim its independence. With independence it became possible to create established ties to global trade.

Singapore has a very successful free-market economy high stability and a very high per capita GDP. The most significant element of the nation's GDP is its exports, relying heavily on electronics, IT products, pharmaceuticals, and financial services.

Singapore is an attractive location for setting up global sourcing operations. It has a welcoming business environment, quality infrastructure, and proximity to Asian customers. This is the primary reason that the sourcing sector is expanding at significant rates.

Outsourcing companies based in Singapore sometimes undertake background screening, although this is usually at the discretion of individual Human Resources (HR) departments. Not all companies carry out such checks for cost reasons. Multinational companies, financial institutions and government organisations, however, generally do carry out pre-employment screening. The prevailing attitude in Singapore is that it is the responsibility of the employer to carry out due diligence on prospective employees, including ensuring that the employer only hires foreign workers with valid work permits.

Data privacy is an extremely new concept in Singapore and the Personal Data Protection Act 2012 has been recently introduced. The legislation is consistent with that of Australia and the EU and will create a framework of Data Protection Rules to commence in mid-2014. The Act controls how 'personal data' is handled. 'Personal data' is defined as:

'data, whether true or not, about an individual who can be identified –
a) from that data; or
b) from that data and other information to which the organisation has or is likely to have access.'

It is clear that 'personal data' will be handled in a number of situations when personnel security measures are undertaken and this Act must be applied whenever necessary.

The Singapore Employment Act does not prohibit an employer from carrying out pre-employment screening, nor does it impose limitations on the types of resource that are available to employers (for example, employment permits or health checks).

Public sources of information available to organisations in the private sector to use in pre-employment screening checks are generally limited to public databases and references provided by the individual. Reference checks may be carried out by the employer's HR staff. It is also common for headhunters to be involved in conducting detailed interviews of referees provided by a prospective employee.

		As regards ongoing personnel security measures, organisations in Singapore are generally permitted to undertake surveillance on the company premises only if the premises and equipment concerned belong to the organisation. If a third party is involved in investigations or monitoring work, it must be a licensed private investigator.
2	Personnel security measures during recruitment	
2.1	Culture of screening	<p>In the private sector the level of pre-employment screening undertaken is generally commensurate with the roles and responsibilities of the individuals concerned. For example, the employer may perform pre-employment screening on prospective employees entering middle or senior management roles, or those who have access to financially sensitive information or assets under control of the organisation.</p> <p>Pre-employment screening for junior employees, where used, is generally limited to verification of previous employment only.</p>
2.2	Major laws and regulations applying to pre-employment screening	<p>The newly introduced Personal Data Protection Act will, for the first time, restrict how employers must deal with any personal data, including that of their prospective, current or past employees. The Rules will apply to all ‘organisations’ with an office in Singapore. Collecting, using and disclosing personal information will require the consent of the individual. Individuals will have the right to bring civil proceedings for any loss or damage suffered from a contravention of the Act. Organisations must appoint at least one data protection officer, who will be responsible for ensuring that the legislation is adhered to. Advisory guidelines to the new regulations are available at www.pdpc.gov.sg/resources/advisory-guidelines.</p> <p>The Employment Act 2008 applies only to the following groups of employees:</p> <ul style="list-style-type: none"> • ‘workmen’ earning a basic monthly salary of S\$4,500 or less • managerial and executive positions earning a basic monthly salary not exceeding S\$4,500 and • other employees earning a basic monthly salary of S\$2,500 or less.

3	Pre-employment checks	
3.1	Identity check	<p>Every Singaporean and Singapore Permanent Resident is issued with a National Identification Card. For foreigners applying to work in Singapore, the common means of identification is the passport. Other identity checks (for Singapore Permanent Residents and foreigners already working in Singapore) would include producing a copy of their last income tax statement or Central Provident Fund statement.</p> <p>An original copy of the ID card should be presented. Under National Residency legislation, a Singaporean citizen and Permanent Resident is required to update their ID card after every change of address.</p> <p>The Central Provident Fund (CPF) is a compulsory national savings scheme for Singaporeans and Permanent Residents. All employees and employers (who contribute a percentage of the employee's salary) must contribute towards an employee's retirement fund. The CPF statement will show:</p> <ul style="list-style-type: none"> • whether an individual has been employed in Singapore • the name(s) of the employers making the contributions and • the individual's residence. <p>Prospective employers can request a candidate to produce the latest CPF statement as part of their recruitment verification records. The individual may refuse to provide this information and there is no legal obligation on them to produce the statement.</p>
3.2	Checks on eligibility to work	<p>Employers in Singapore seeking to employ foreign nationals must apply to the Ministry of Manpower for a work permit before the foreigner can commence work. An employer is not able to access previous work permit or employment applications relating to a prospective employee, nor find out whether previous permits have been revoked. The employer must submit an application for such permits and await approval from the Ministry of Manpower. A new work permit is required for each separate employment.</p>
3.3	Residency checks	<p>The prospective employee's residency is stated on their National Identity Card and also, where applicable, their application for an employment permit. A number of commercial data aggregators provide services to verify identity and residency that are based on data sourced from a combination of some or all of:</p> <ul style="list-style-type: none"> • business interest records, and • litigation and bankruptcy records. <p>The main commercial providers of this type of data in Singapore are:</p> <ul style="list-style-type: none"> • DP Information Pte Ltd (more commonly known as Questnet – www.questnet.sg) and • Biznet (owned by CrimsonLogic – www.biznet-global.com) who have agreements with relevant government departments to provide up-to-date information.

		<p>It is also possible to visit:</p> <ul style="list-style-type: none"> • the company registry, ACRA (www.acra.gov.sg) to obtain information on business interests of any individual, and • the Insolvency and Trustee’s Office (www.ipto.gov.sg) to obtain bankruptcy information. <p>Apart from the information listed on the National Identity Card and employment documents, it is not possible for an employer to access residency data. For example, electoral roll data in Singapore is not a matter of public record.</p>
3.4	Criminal record checks	<p>Name of certificate</p> <p>Certificate of Clearance (COC).</p> <p>Department that holds records</p> <p>Criminal Investigation Department of the Singapore Police Force.</p> <p>Where to apply within country</p> <p>Criminal Investigation Department, Singapore Police Force, Block D, Police Cantonment Complex, #02–07/08, 391 New Bridge Road, Singapore 088762.</p> <p>Telephone: +65 (0)6435 0000/ +65 (0) 6557 3985 Email: SPF_CID_COC@spf.gov.sg Website: www.spf.gov.sg/epc/cert_issued.htm</p> <p>How to apply within country</p> <p>In person to the address above with the following:</p> <ul style="list-style-type: none"> • completed application form (available at www.spf.gov.sg/epc/cert_issued.htm) • a set of the individual’s fingerprints (taken at the COC office at the time of application) • a photocopy of a valid passport issued to the individual • two recent passport-sized photographs and • a photocopy of a document from relevant consulate/immigration authority/government body/employer to establish that the certificate is required. All documents must be translated into English if necessary. <p>Who can apply</p> <p>Individuals (Singaporean citizens only) and third parties (with the applicant’s consent).</p> <p>Non-citizens may make an appeal for a COC by submitting the appeal in writing, supported by relevant documents such as a letter from the requesting authority and documentary proof of stay in Singapore. Appeals are treated on a case-by-case basis and processing time is approximately 15 working days.</p>

		<p>Cost</p> <p>The cost is SG\$45.</p> <p>Payment</p> <p>In person – payment can be made in cash, by NETS, cash card or credit card (Visa/Mastercard).</p> <p>By post – bank draft made payable to ‘Head Criminal Records CID’ in Singapore dollars through a financial institution based in Singapore. In addition to the certificate fee, a postage fee of SG\$5 must be included if the COC is to be sent to an overseas address.</p> <p>Turnaround</p> <p>The turnaround time is approximately ten working days.</p> <p>A fast-track application can be requested when submitting the application. All requests are dealt with case by case.</p> <p>Legislation</p> <p>Singapore Penal Code (Chapter 224) 30 November 2008.</p> <p>Further information can be obtained from the CPNI guidance on <i>Overseas Criminal Record Checks</i> which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>
3.5	Education checks	<p>Education checks are often required by employees to establish that a prospective employee attended the educational establishments claimed. Typical information provided is:</p> <ul style="list-style-type: none"> • dates of joining and leaving the educational institution • subject of study • courses (college, university) • degree and • final mark. <p>In many cases, this information is confirmed only and not volunteered.</p> <p>Application for such information must be made in writing and provide all known information, e.g. full name, date of birth, subject of study. Many organisations have a standard process for dealing with reference enquiries. The consent of the individual is required.</p> <p>Employers usually require candidates to provide original testimonials, degrees/diplomas and results slips for verification. Depending on the policies of the employer, further verification may be requested from the educational institution, but this would require the consent of the individual.</p>

<p>3.6</p>	<p>Qualification checks</p>	<p>Verification of qualifications (academic or professional) is a regular part of pre-employment screening, if this is undertaken.</p> <p>Typical information confirmed is:</p> <ul style="list-style-type: none"> • dates of joining and leaving the educational institution or professional body • membership status (professional body) and • status and type of qualification. <p>In many cases, all known information must be provided. The institution will confirm information, although it will not volunteer any data. Often questions regarding the character of an individual will not be answered in writing by educational institutions, although a verbal character reference might be obtained from a tutor or professor who knows the individual.</p> <p>Fake documentation is widespread and it is regularly reported that a proportion of candidates lie about or exaggerate qualifications. Attendance at an educational establishment does not prove that the individual graduated from that establishment.</p> <p>It is also important to verify that an individual is an active member of a professional body and has not left nor been ejected from membership.</p>
<p>3.7</p>	<p>Employment references</p>	<p>It is normal for employers to provide references. These may confirm basic information such as dates of employment, positions held and reason for leaving. They do not necessarily include character references although employers in Singapore generally provide neutral or positive feedback regarding the prospective employee's work attitude at the request of the employee. When requesting references, employers in Singapore should refrain from asking questions relating to race, as Singapore is a multiracial society, or questions about family situations and the impact on the candidate's ability to work. Most employers will not provide information on salaries, sickness record, performance records or parental leave. Reference requests are made directly to previous/current employers. The consent of the individual is required.</p> <p>Character references are not always given by previous employers. They may offer only verification of basic details of employment history and reason(s) for leaving. Character references from persons of standing in the Singapore community may be sought and there is no legal restriction. Care should be exercised to ensure that the referees are independent of the candidate (i.e. are not relatives).</p>

3.8	Financial/ credit checks	<p>These checks are typically used for persons applying for more senior roles and, in particular, those involving access to financial systems or controls. They may be undertaken at the pre-employment stage, on an ongoing basis, or where suspicions/concerns arise. A number of privately owned, data aggregating firms provide credit data. These records can be accessed online by employers, who must register with the provider of credit information. Costs depend on the provider and the subscription type. Requests for credit information will leave a record on the individual's credit file.</p> <p>Credit reports from Singapore's Credit Bureau (which is technically the most comprehensive source of information) are intended for use by financial institutions and are not available to third parties without the consent of the individual. Where it is necessary to gain access to the report, employers must ask the individual to request the report from the Credit Bureau. There are privately owned databases (such as Questnet) which provide credit reports on individuals but such information is proprietary and they do not guarantee accuracy.</p> <p>Credit records can be subject to error or omission. Individuals can apply to the credit bureau concerned to have their record amended if they believe it to be inaccurate. All credit bureaux have established appeals processes.</p>
3.9	Substance abuse screening	<p>There are no legal restrictions on the use of substance abuse screening in Singapore. The explicit consent of the individual would be required. Most employers require prospective employees to attend a medical check at a designated clinic after they have been offered employment. A substance abuse check can be undertaken at this stage.</p>
3.10	Occupational health checks	<p>There are no legal restrictions on the use of occupational health checks in Singapore. The explicit consent of the individual would be required. However it is usual for employers in Singapore to request that the prospective employee obtain a health check report and provide it to the employer.</p>

4	Personnel security measures during employment	
4.1	Legal requirements	<p>The new Personal Data Protection Act has introduced new rules regarding data privacy which should be applied when dealing with employee’s personal information.</p> <p>Private surveillance may only be carried out by licensed private investigators. Private investigators are regulated under the Private Security Industry Act 2008.</p> <p>The Singapore Constitution is based on the British system. It contains no explicit right to privacy. The High Court has ruled that personal information may be protected from disclosure under a duty of confidence.</p> <p>Computer networks in Singapore are protected through three major bills:</p> <ul style="list-style-type: none"> • The Electronic Transactions Act imposes a duty of confidentiality on records obtained under it. Penalties under the Act include a maximum fine of SG\$50,000 and a 12-month jail sentence for unauthorised disclosure of records. The Act provides the police with a wide range of powers to investigate internet-related crimes. They may search any computer and require disclosure of documents without a warrant in relation to any offence committed under the act. Defendants have a right to judicial review of cases in which police searches are conducted. • The Computer Misuse Act prohibits the unauthorised use of, access to, and modification of computer data. The Act also provides the police with additional powers of investigation. Under the Act it is an offence to refuse to assist the police in an investigation and law enforcement agencies are granted a broad power to access data and encrypted material when conducting an investigation. This power of access requires the consent of the Public Prosecutor. • The Info-communications Development Authority of Singapore Act incorporated the Authority ‘to establish and maintain, to the extent permitted by any law, standards and codes for the monitoring and regulation of such aspects of information and communications technology data privacy and protection as the Authority thinks fit’. Under this Act the Singapore government has wide powers to monitor any activity that it considers is a ‘threat to national security’. <p>Employer monitoring of employee phone calls, emails, and internet usage has previously been permissible under Singapore law. Under Singapore property law, workplace email, telephone and computer contents are the property of the employer. However, care must be exercised in the use of such measure since the introduction of the Data Protection Rules.</p>

		<p>In Singapore, the privacy of bank customers is protected under the Banking Act. Section 47 of the Act governs banking secrecy. The Act prevents disclosure of information without the explicit consent of the customer. There are certain exceptions to this, for example in relation to requirements to report suspicions of money-laundering activities. The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, commonly known as CDSA, is the primary legislation enacted to combat money laundering in Singapore. Singapore also has an Official Secrets Act which relates to the security of official secrets.</p>
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	<p>The Employment Act details the rights and duties of both employers and employees.</p> <p>If an employee breaches his or her employment contract, is found guilty of misconduct or poor performance, the employer reserves the right to dismiss the employee.</p>
4.4	Local legislation that specifically governs the rights of the employee	<p>The Employment Act covers the rights of certain groups of employees. This relates to the basic terms and working conditions of the employees. There is no specific provision that impacts on personnel security except that the employer has to ensure a safe and healthy workplace for the employees. Were employees in Singapore to challenge an employer's use of security procedures described in this report, recourse might be available through civil courts.</p> <p>Only employees who are covered under the Employment Act have recourse to unfair dismissal provisions under the Act. The recourse available to employees who are not covered under the Act is through civil litigation or a trade union, if they belong to one.</p>
4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	None stated.
4.6	What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?	Terminations must follow the terms and conditions included in the employment contract. Unfair dismissal claims can be made under the Employment Act although this Act only covers certain employees; other employees would have to make any claim through their trade union or via civil litigation.

4.7

**Availability
of security
measures**

Monitoring by the employer of employee phone calls, emails and internet usage has been permissible under Singapore law. Workplace email, telephone and computer contents are the property of the employer. However, care should be exercised with regard to the Data Protection Rules introduced in 2014, which control how 'personal data' can be handled. 'Personal data' are defined as:

'data, whether true or not, about an individual who can be identified —

- a) from that data; or
- b) from that data and other information to which the organisation has or is likely to have access'.

Restriction of access to premises

This is permitted so long as the party restricting access has a legal right to do so (i.e. is the owner or tenant of the premises).

Restriction of access to certain rooms/zones on the premises

This is permitted so long as the party restricting access has a legal right to do so (i.e. is the owner or tenant of the premises).

Physical screening (on entry/exit)

Such screening is typically undertaken at the entrances to commercial buildings.

Prohibition of removal of data from the premises (hard-copy)

Although there is no specific data protection legislation in Singapore, information and documents created during an individual's employment belong to the employer and employees can be prevented from removing such data from the employer's premises.

Prohibition of removal of data from the premises (electronic)

See above.

Visual surveillance (CCTV or other cameras), either overt or covert

CCTV is commonly used in Singapore in public spaces such as lifts, offices or shops and also in places of work.

Overt monitoring of access to IT and other equipment

IT equipment (such as computers or servers) and email can be monitored by an employer. There is no privacy legislation prohibiting such measures but it is preferable that the employer makes it known to all employees that such measures are being employed, and this may form part of the employment contract.

Covert monitoring of access to IT and other equipment

See above.

Reporting hotlines (anonymous)

There is no legislation prohibiting the use of reporting hotlines in Singapore. These are commonly used by employers in Singapore. The procedures for receiving anonymous/confidential reports through such hotlines are usually communicated by employers to employees via corporate governance and HR policies.

		<p>Reporting hotlines (confidential)</p> <p>See above. Confidential hotlines are preferred to anonymous hotlines. In addition, it is good practice for a company to disclose the identity of the organisation manning its hotline.</p> <p>Use of alerts/automated warning systems to identify unusual employee behaviour (out-of-hours activities, duplicate payments)</p> <p>This security option is available to employers in Singapore.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>Monitoring of communications is permissible, provided the medium for such communications belongs to the employer. Organisations should preferably inform employees that monitoring procedures may be carried out. This could be done in the employment contract.</p>
4.8	Formal investigations	<p>Is there a licensing regime covering investigators?</p> <p>In Singapore, a private investigator must be licensed and is regulated under the Private Security Industry Act that was enacted in September 2007 to enable and put in place an enhanced regulatory framework. Under the Act, a ‘private investigator’ means any individual who, for reward, carries out any of the following functions:</p> <ul style="list-style-type: none"> • obtaining and giving information about any person • searching for missing persons • obtaining and giving information as to the cause and origin of or responsibility for any fire, libel, loss or accident or any damage to real or personal property • obtaining and giving information as to the location or recovery of lost or stolen property or • obtaining evidence to be used in any civil or criminal proceedings. <p>Physical surveillance (overt or covert)</p> <p>There are no specific laws that prohibit the use of physical surveillance (overt and covert) by the police or licensed private investigators.</p> <p>Electronic surveillance (e.g. tracking devices)</p> <p>There are no specific laws that prohibit the use of physical surveillance (overt and covert) by the police or licensed private investigators.</p> <p>Visual and communication surveillance (using cameras, video or CCTV)</p> <p>CCTV is widely used in many public places including commercial buildings and private homes.</p> <p>Communication intercept (including oral, written and electronic communication including bugging devices)</p> <p>Many organisations, such as government departments and stockbroking firms, maintain tape recordings of telephone conversations of their staff as a matter of routine. The reasons for such recording will depend on the employee’s role. Organisations that adopt this practice will generally notify employees of the use of recording and will explain the rationale for its use.</p>

Computer or database surveillance (using either hardware or software tools, including forensic tools)

In private investigations, it is possible to carry out computer or database surveillance if the equipment belongs to the organisation.

Formal interviews of staff

In Singapore, only the police and relevant government authorities have the powers to compel interviews for the purposes of a criminal investigation under the law. Interviews undertaken by any other party for investigative purposes are considered voluntary and would require consent from the individual in question. An organisation's HR policies may require the mandatory assistance of an employee (either through interviews or physical searches) in an internal investigation.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

Financial transactional data and credit card activity are not available to third parties under the Banking Act. However, organisations that deem it necessary to monitor financial transaction data and the credit card activity of their employees would provide for such measures under their HR policies and employment contract.

Search and seizure of evidence, whether electronic or physical (overt or covert)

For the purposes of carrying out criminal investigations, the police have the powers to search and seize evidence (both overt and covert) relating to individuals and employers.

For private investigations that they carry out themselves, organisations only have access to evidence or information that belongs to them. For example, the organisation can obtain physical and electronic data from computers that belong to it. Whether electronic information is obtained overtly or covertly would depend on the nature of the matter and whether there is a risk that the evidence might be tampered with by the subject(s).

Such measures are usually undertaken by a specialist (e.g. a forensic technology specialist), as the securing of electronic evidence must be carried out to the level acceptable in a criminal investigation. Whether overt or covert searches for physical evidence are carried out in the workplace would also depend on the subject matter.

Is it either usual or necessary to involve the police in investigations?

It is necessary to involve the police as soon as possible if there is a suspicion that a criminal offence has been committed.

However, it is usual for employers to either carry out internal investigations or engage third parties (such as forensic accountants or private investigators) to perform investigations in commercial cases to establish prima facie evidence before making any report to the police.

Where matters involve internal disciplinary matters or corporate governance issues, there is no need to involve the police.

		<p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>In Singapore, involving law enforcement authorities depends on whether there is sufficient <i>prima facie</i> evidence to lodge a case. This is especially relevant in commercial cases where the authorities expect an organisation to undertake its own investigations (either on its own or using an independent third party) to gather the facts and <i>prima facie</i> evidence before lodging a complaint.</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>Section 39 of the CDSA Act requires anyone to report to a Suspicious Transaction Reporting Officer as soon as is reasonably practicable where he or she knows or has reasonable grounds to suspect that any property:</p> <ul style="list-style-type: none"> • in whole or in part, directly or indirectly, represents the proceeds of • was used in connection with or • is intended to be used in connection with <p>any conduct that may constitute drug trafficking or criminal behaviour and the information or matter on which the knowledge or suspicion is based came to his or her attention in the course of a trade, profession, business or employment.</p> <p>Other legal considerations not covered above</p> <p>Employers must consider whether they might be subject to civil action by third parties if they do not undertake an internal investigation, where they breach certain reporting obligations (such as to the stock exchange or relevant government authorities).</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

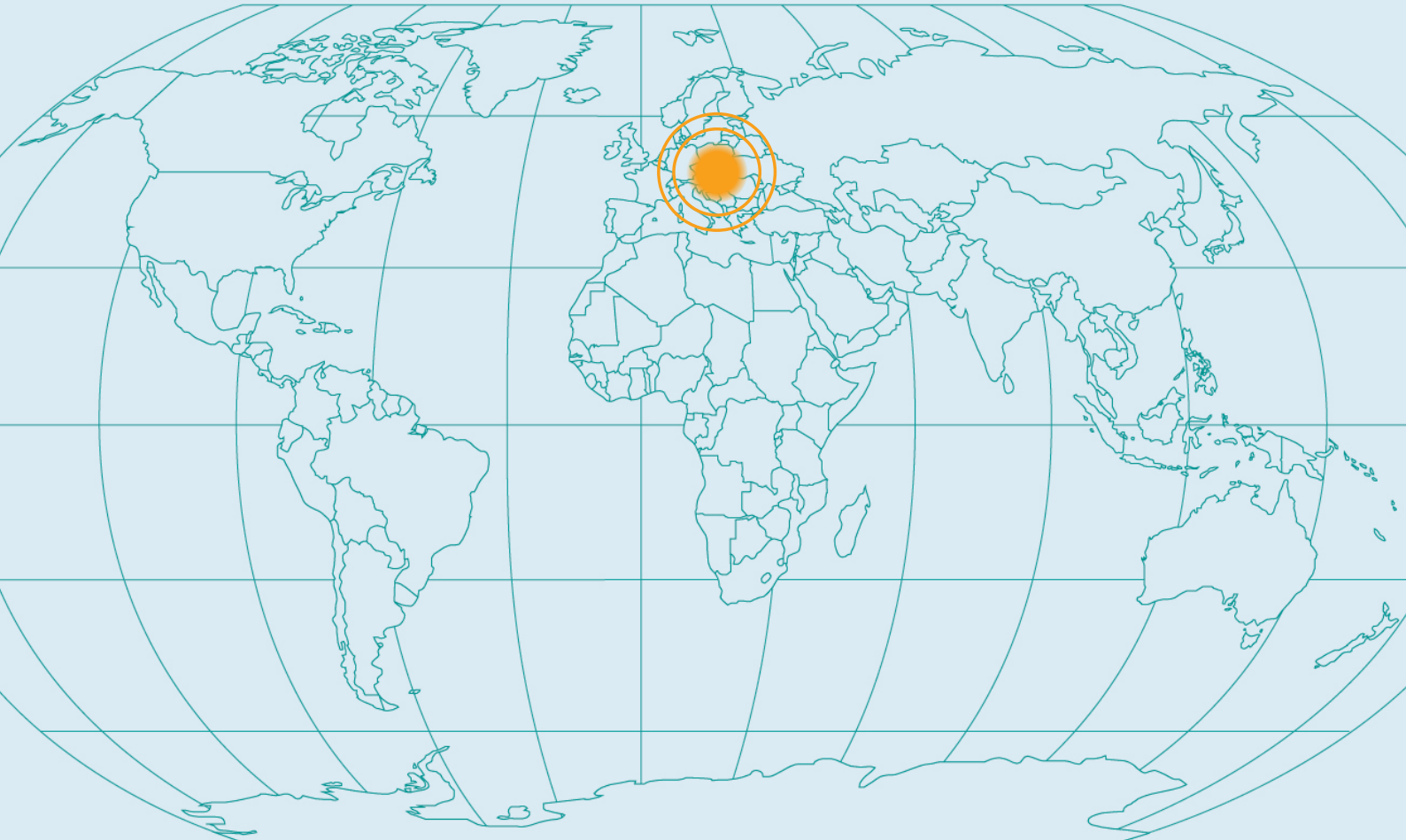
CPNI

Centre for the Protection
of National Infrastructure

SECURITY WATCHDOG
Part of Capita plc

Slovakia

Personnel Security in Offshore Centres



Slovakia

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

1	Introduction	<p>Slovakia is a popular location for ‘near-shoring’ operations within the Central and Eastern Europe region. It has benefited from opportunities for outsourced operations from Western European companies in particular.</p> <p>Slovakia offers a number of advantages such as:</p> <ul style="list-style-type: none"> • a workforce that is proficient and skilled in European languages, in particular English and German • a workforce that is highly educated, particularly in mathematics, sciences and information technology and • close cultural and geographical proximity to Western Europe. <p>In addition, Slovakia’s membership of the European Union (EU) means that it has adopted laws and regulations that are consistent with other European countries (such as data protection legislation). Slovakia has particular expertise in the mobile telecommunications and internet sectors. These advantages should be set against other factors such as a relatively small population and increasing wage costs.</p>
2 Personnel security measures during recruitment		
2.1	Culture of screening	<p>In Slovakia pre-employment screening is generally undertaken at the discretion of the individual employer. Employers usually adopt the following employment screening procedures:</p> <ul style="list-style-type: none"> • the Human Resources department requires a criminal records check to be submitted on the first day of employment – in many public sector and larger private sector organisations, provision of a criminal record check is a condition of employment • verification of any higher education qualifications not checked during the pre- employment screening process – organisations may require the employee to provide a copy of their diploma certificate on the first day of employment and provision of this document is also, generally, a condition of employment • verification of any professional qualifications claimed is at the discretion of the employer; many employers require new employees to provide official confirmation of professional qualifications held, and • occupational health checks are commonly applied to individuals entering employment with public authorities. <p>The level of pre-employment screening is generally commensurate with the role and responsibilities of the individual concerned. For example, an individual with access to sensitive financial data would generally be subject to higher levels of screening than one who would not have such access. Senior management team members may be subject to enhanced screening procedures.</p> <p>There are no minimum requirements for pre-employment screening in Slovakia.</p>

2.2

Major laws and regulations applying to pre-employment screening

The major laws and regulations that apply to pre-employment security procedures in Slovakia are as follows:

- The **Anti-discrimination Act No. 365/2004**, which prohibits discrimination on the grounds of:
 - gender
 - religion
 - ethnic origin
 - nationality
 - health
 - age
 - sexual orientation
 - marital status
 - family status
 - skin colour
 - language
 - political opinion or status
 - national or social origin
 - property
 - trade union activity or
 - other status.

The Act requires equal treatment in these areas during the process of application and selection for employment. However an employer may require specific health checks for certain positions or specify general health status requirements.

- The **Act No 122/2013 Coll. on Protection of Personal Data** implements the **EU Data Protection Directive (95/46/EU)** and regulates the way in which personal data (including those collected in the course of an investigation on behalf of the employer) can be gathered, retained, stored and destroyed. The Act allows personal data obtained during an investigation to be retained for as long as is necessary for the duration of the purposes they are used for. The organisation must be able to justify, by reference to the nature of an incident or suspicion, or the likelihood of appeal, why continued retention of the data is necessary. Information collected during investigations should normally be held for the duration of the purpose for which it was collected. An organisation may keep personal data only with the approval of the individual concerned. The Act is enforced by the **Office for Personal Data Protection** (*Úrad na ochranu osobných údajov Slovenskej republiky*).
- The **Act on Banks No. 483/2001** covers branch offices of foreign banks, amongst other organisations, and lays down requirements for particular positions, for example compliance department employees. Other requirements may be defined in other sector-specific regulations.
- The Act on Social Insurance provides rules for pension calculation and these relate to documents necessary to attest previous experience.

In view of the potential legal complexities in relation to specific circumstances, further legal guidance should be sought in individual cases.

3	Pre-employment checks	
3.1	Identity check	<p>It is regular practice to undertake checks on an individual's identity (given name, date of birth, parents' names, addresses).</p> <p>If an individual loses his or her identification documents, the police may issue a temporary certificate.</p> <p>In Slovakia there are no legal prohibitions on undertaking identity checks. The preferred forms of identification include the following:</p> <ul style="list-style-type: none"> • passport • drivers' licence (in limited cases) or • National Identity Card. <p>Marriage, birth or adoption certificates and tax notifications offer a lower level of identity verification.</p> <p>It is common practice in Slovakia for employers to verify the identity of prospective employees by reference either to a passport or an ID card.</p>
3.2	Checks on eligibility to work	<p>Such checks are required if the individual is not a national of the EEA with the right to work in Slovakia.</p> <p>Typically, employers in Slovakia assist employees to obtain work permits as part of their pre-employment security procedures.</p> <p>Detailed guidance on Slovak work permit procedures is available from the Labour Office; see www.employment.gov.sk. The issue of work permits in Slovakia is governed by Act 5/2004 Coll. on Employment Services.</p>
3.3	Residency checks	<p>Residency checks on current and former addresses may be undertaken at the discretion of the employer.</p> <p>This information is usually requested by the employer directly, although it might engage a third party to undertake such checks.</p> <p>Post Office data, telephone subscriber data and utility company data can be requested from a potential employee. An employer may also use the Land Cadastre database to check ownership of properties; see https://www.katasterportal.sk/kapor/.</p> <p>A number of commercial organisations (for example, private investigators) can provide services to verify identity and residency. These checks are based on data sourced from a combination of some or all of: Post Office, telephone subscriber, utility company and credit bureau.</p> <p>Employers should be aware that telephone subscriber data, utility information and commercial data may be inaccurate, out of date or incomplete.</p>

<p>3.4</p>	<p>Criminal record checks</p>	<p>Name of certificate</p> <p>Extract from the Criminal Record (Výpis z registra trestov). Full Copy of Criminal Record (Odpis registra trestov).</p> <p>Department that holds records</p> <p>Criminal Register of General Prosecutor's Office of the Slovak Republic (Register trestov Generálnej prokuratúry Slovenskej republiky).</p> <p>Where to apply within country</p> <p>Register of Convictions, Register trestov Generálnej prokuratúry Slovenskej republiky, Kvetná 13, P.O. Box 147, 814 23 Bratislava, Slovak Republic.</p> <p>Telephone: +421 (0)2554 25 649 /+421 (0)2554 10 817 Web: www.genpro.gov.sk/register-of-convictions-1389.html</p> <p>How to apply within country</p> <p>Applications can be made at every municipal registrar, prosecutor's office and at the headquarters of the Criminal Register.</p> <p>The individual can apply by post or in person and must provide the following:</p> <ul style="list-style-type: none"> • application form • Slovak ID card/passport and • birth certificate. <p>All documents must be submitted in the Slovak language. If they are in a different language they must be officially translated for submission. Only originals of documents will be accepted.</p> <p>Who can apply</p> <p>Individuals and persons authorised by the individual.</p> <p>Cost</p> <p>€4</p> <p>Payment</p> <ul style="list-style-type: none"> • Cash • personal cheque or • cash via special machine (at Criminal Register head office only). <p>Turnaround</p> <ul style="list-style-type: none"> • Instantly, if the request is made in person at a location that has online access • one or two days for requests made by post, with postage time on top; however, • there is no system in place for fast-track cases.
-------------------	--------------------------------------	--

		<p>Legislation</p> <ul style="list-style-type: none"> • Act 330/2007 Coll. Criminal Register • Act 300/2005 Coll. Criminal Code • Act 301/2005 Coll. Criminal Procedure • Act 215/2004 Coll. Protection of Classified Information and • Act 122/2013 Coll. Data Privacy. <p>Further information can be obtained from the CPNI guidance on Overseas Criminal Record Checks which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>
3.5	Education checks	<p>Education checks are often required by employers to establish that a prospective employee has attended the educational establishments claimed.</p> <p>Typical information provided is dates of joining and leaving the educational institution (school, university), subject of study and degree. In the majority of cases, this information is provided by the employee in the form of qualification certificates and is not confirmed by educational institutions. Employers can ask for confirmation from the educational institution, however.</p> <p>Often questions regarding the character of an individual and other personal information will not be answered by educational institutions.</p> <p>Typically, results of education checks are accompanied by the official stamp of the educational institution concerned. This ensures that an employer can verify the authenticity of the information provided.</p> <p>Under Article 6 of the Anti-discrimination Act (as amended), it is illegal to discriminate on the grounds set out in Section 2.2. The act requires equal treatment in all of these areas during the application for employment and selection process.</p> <p>The consent of the individual is generally required to conduct such checks.</p> <p>In practice, the individual normally requests and collects such information, although he or she might ask the educational establishment to inform the prospective employer directly.</p>
3.6	Qualification checks	<p>Checks are often required by employers to establish that a prospective employee has obtained any qualifications claimed.</p> <p>Typical information provided is dates of joining and leaving the educational institution or professional body, membership status and status and type of qualification. In the majority of cases, this information is provided by the employee who requests confirmation from the professional institution.</p>

		<p>Generally questions regarding the character of an individual will not be answered by educational institutions. The requirements of the Anti-discrimination Act (as detailed in Section 2.2) also apply to qualification checks. Verification is generally undertaken by application directly to the educational establishment or the professional body. Most such bodies have standard processes for dealing with reference enquiries. The consent of the individual is generally required.</p> <p>Most professional bodies in Slovakia issue directories of members. The accuracy of professional qualifications can be verified directly with the professional body. Many Slovak professional organisations maintain lists of members online (for example, public accountants, advocates, notaries, tax advisers, construction engineers, executors, court experts, actuaries, architects, mediators, etc). The consent of the individual is not generally required as this is published information.</p> <p>It is important to verify that an individual is an active member of a professional body and has not left nor been ejected from membership.</p>
3.7	Employment references	<p>It is rare for employers to comment on the character of a former employee. Also, most employers will not provide information on salaries, sickness record or parental leave. Where the previous employer is not well known, it may be necessary to undertake additional checks to verify its existence/background.</p> <p>Some employers require references from previous employers. Many employers do not provide written character references or comments on performance. Taking up character references from previous employers is at the discretion of individual organisations. Written references may be verified over the phone if necessary.</p> <p>The conditions of the Anti-discrimination Act (as detailed in Section 2.2) also apply to qualification checks.</p> <p>Previous employers typically provide a practice certificate (<i>zapocet rokov</i>) and confirmation of income due on the annual tax return. Employers may also provide details of the previous salary. The practice certificate states the dates of employment and of any sick leave in the previous year.</p> <p>Character references usually involve persons of standing (e.g. police officers, professionals) who have known the individual for a period of time.</p> <p>An employer can request a reference from a professional body, for example, the Slovakian Medical Chamber, the Slovakian Pharmaceutical Chamber, the Slovakian Chamber of Tax Advisers, etc. However this is not common practice in Slovakia.</p>

3.8	Financial/ credit checks	<p>Although rare in Slovakia these checks may be made in more senior roles, in relation to those involved in the financial sector and in particular individuals with access to financial systems or controls. Financial/credit checks may be undertaken during the pre-employment screening stage, on an ongoing basis or when suspicions or concerns arise.</p> <p>There are no legal restrictions on the use of financial/credit checks, although the consent of the individual is generally required to conduct a credit check. Some of the leading organisations offering such services include the Slovak Banking Credit Bureau and Credit Info (typically, however, these organisations focus on corporate entities).</p>
3.9	Substance abuse screening	<p>Screening for substance abuse is not widespread. Where it is used, it may be part of ongoing security: either random screening or where there is suspicion of substance abuse.</p> <p>Employers have the right to ask for a general health check to be performed by a doctor before employment begins. Employees entering particular positions (for example hospital workers, social workers, catering industry workers) are obliged to undertake specific health checks.</p> <p>An employer may request that a health check covers substance abuse screening. Substance abuse screening is likely to be a sensitive topic and would normally only be applied in specific situations (e.g. the prospective employee presents a heightened level of risk to the employer because of prospective position/access rights, etc).</p> <p>There are no specific legal restrictions, although the explicit consent of the individual would be required.</p>
3.10	Occupational health checks	<p>This type of check may be required where the individual will be employed in situations where health issues could cause physical risks to other individuals (e.g. train driver, forklift truck operator, medical practitioner).</p> <p>Entrance health checks are common practice but normally within the induction period and not as part of the pre-employment screening process.</p> <p>The Anti-Discrimination Act prohibits discrimination based on health, age or other status. It requires equal treatment in these areas during the process of application and selection for employment. However an employer may require specific health checks for particular positions or specify general health status requirements.</p>

4	Personnel security measures during employment	
4.1	Legal requirements	<p>The major laws and regulations that affect an employer’s ability to carry on ongoing personnel security measures are :</p> <ul style="list-style-type: none"> • rights to personal privacy are set out in the Constitution of the Slovak Republic, Act No. 460/1992 and the Civil Code, Act No. 40/1964; under the Constitution and the European Convention for the Protection of Human Rights and Fundamental Freedoms, organisations should take into account the importance of respecting employees’ right to a private and family life • the Act No 122/2013 Coll. on Protection of Personal Data (see Section 2.2). • the Anti-discrimination Act (see Section 2.2). • the Private Security Act No 473/2005 defines security service, detective service (agency) and security advisory roles and covers asset security, personal security, asset tracing, tracing and monitoring of individuals, information and data gathering (regarding criminal evidence in the court), etc – information obtained by registered detective agencies may be used in legal proceedings • the Electronic Communications Act No. 610/2011 implements the EU Directive on Privacy and Electronic Communications (2002/58/EC) and regulates electronic communications, including communication intercepts • the Labour Code (Act No. 311/2001) (amended 2011), under which an employer has the right to control the work performance of employees in the workplace, to regulate the use of its own property (i.e. computers and telephones) and to limit the use of private communications using its own equipment, although in practice this is rare. • the Anti-Money Laundering Act No. 297/2008 Coll imposes obligations on individuals in the regulated sector to report suspicions or knowledge of money laundering activities to the police.
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	<p>The rights of the employer and employee are governed by the Labour Code (see Section 4.1). Specific rights of the employer may be protected by intellectual property rights, and rights imposed under the employment contract. The Labour Code defines types of employment, working time, free time, social policies of the organisation, compensation arrangements, collective bodies, company policies, etc.</p> <p>Legal action for breach of contract may restrain an employee from disclosing client-confidential information.</p>
4.4	Local legislation that specifically governs the rights of the employee	<p>The rights of the employee are also governed by the Labour Code (see Section 4.1). In addition, employees may be represented by a local trade union. There are around 350,000 trade unionists in the Slovak Republic. The dominant trade union confederation is the Konfederácie odborových zväzov Slovenskej republiky (KOZ SR).</p>

4.5	<p>What avenues are open to employees who seek to challenge an employer's use of security procedures?</p>	<p>Individuals may bring a claim against their employer under the legislation detailed in Section 4.1. Additionally, many employers have established complaints procedures under their employment contracts, which may allow local trade unions to represent the employee. Human rights violations can be appealed to the Slovakian Human Rights Ombudsman (the Public Defender of Rights).</p>
4.6	<p>What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?</p>	<p>Dismissal of employees in Slovakia is governed by the Labour Code (see Section 4.1). An employee may be dismissed either individually or through a collective redundancy programme.</p> <p>Where an employee is subject to disciplinary proceedings a two-step dismissal process must be followed. Failure to follow the statutory procedures prior to dismissal will render the dismissal automatically unfair and may lead to a claim for compensation against the employer.</p> <p>Under Article 63(5) of the Labour Code the two main stages of the dismissal process are:</p> <ul style="list-style-type: none"> • issuing a written warning to the employee informing him/her of the reasons for dismissal and • an appeals process (giving the employee an opportunity to challenge the dismissal), which must occur within six months of the written warning. <p>The Labour Code details the situations in which an employer can dismiss an employee. The employer may issue a warning and, if the employee fails to address the issues, initiate dismissal. According to Article 63(1) of the Labour Code, 'an employer may give notice to an employee only for the following reasons: an employee does not satisfactorily fulfil the work tasks, and the employer has in the preceding six months challenged him in writing to rectify the insufficiencies, and the employee failed to do so within a reasonable period of time'.</p> <p>For further details of the Labour Code provisions see www.employment.gov.sk/en/labour-employment/labour-relations/labour-code.html (Articles 61 to 70).</p>
4.7	<p>Availability of security measures</p>	<p>Restriction of access to premises</p> <p>The Private Security Act governs the rights of security providers to restrict access to premises, undertake physical screening measures, use surveillance, etc (this covers companies that maintain internal security departments, which must hold a licence to undertake guarding duties).</p> <p>Organisations in Slovakia apply different types of security measures to restrict access to premises:</p> <ul style="list-style-type: none"> • large manufacturing companies typically employ security service organisations to conduct physical checks of individuals and vehicles while • public agencies and larger organisations such as banks maintain logs of persons entering/leaving buildings, who was visited, time and ID number.

Restriction of access to certain rooms/zones on the premises

See above. Typically, restricted areas include archives, warehouses or sensitive information technology equipment.

Physical screening (on entry/exit)

See 'Restriction of access to premises' above.

Prohibition of removal of data from the premises (hard-copy)

The Private Security Act gives professional security service providers rights in protecting assets. The Protection of Personal Data Act governs personal data. Removal of data from the premises/from secure systems is loosely defined in the Labour Code.

In employee contracts employers generally place restrictions on the removal of data.

Prohibition of removal of data from the premises (electronic)

It is up to the employer to define confidential data according to the Commercial Code and protect it in line with relevant legislation.

The Protection of Personal Data Act governs protection of personal data. Removal of data from employers' premises or from secure systems is not well defined in the Labour Code, so the employer usually sets up any prohibition in its employee contract.

Visual surveillance (CCTV or other cameras), either overt or covert

Visual surveillance is regulated by the Human Rights Convention and the Private Security Act. CCTV is commonly used in Slovakia to cover critical infrastructure points (e.g. perimeters). As its use is subject to other laws, organisations may wish to seek legal advice on its specific use.

Overt monitoring of access to IT and other equipment

In Slovakia employers may monitor access to equipment, subject to the provisions of the Protection of Personal Data Act on personal privacy. Generally, an employer has a right to review access to information held on its own systems or equipment.

Covert monitoring of access to IT and other equipment

See above.

Reporting hotlines (anonymous)

Often the use of reporting hotlines, while legal, is not considered socially acceptable, and so this is not a widely used measure.

Individuals are required to report certain crimes listed in the Slovakian Penal Code, including domestic and foreign bribery. Any person who obtains 'any reliable information' regarding such crimes must report this immediately to 'a prosecutor, investigator or a police body'. Failure to report is punishable by imprisonment for up to three years. Under the Penal Code, a person need not report such concerns if he/she is bound by a non-disclosure obligation laid down by law.

		<p>Section 13 of the Labour Code states: ‘In the workplace, nobody may be persecuted or otherwise sanctioned in the performance of labour law relations for submitting a complaint, charge or proposal for the beginning of criminal prosecution against another employee or the employer.’</p> <p>Aggrieved whistleblowers may seek protection from a court. There are no specific legal requirements to provide a whistleblower’s identity.</p> <p>Reporting hotlines (confidential)</p> <p>See above</p> <p>Use of alerts/automated warning systems to identify unusual employee behaviour (out-of-hours activities, duplicate payments)</p> <p>In Slovakia employers may monitor access to equipment, subject to the provisions of the Protection of Personal Data Act on personal privacy. Generally, an employer has a right to review access to information held on its own equipment. An employer’s use of such systems would generally be considered acceptable, provided that it is proportionate to the risks faced.</p> <p>Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)</p> <p>Where monitoring involves the collection of personal data, the Protection of Personal Data Act requires that such data are collected lawfully and processed in a fair and proper way. Covert monitoring may be undertaken only in exceptional cases (provisions are set out in the s. 55 of the Electronic Communications Act, which can be found at http://teleoff.gov.sk/data/files/22211.pdf). Monitoring of employee communications using the employer’s equipment is legal, although the policy on monitoring should be clearly communicated to employees.</p> <p>Further information is available from the Ministry of Labour, Social Affairs and the Family (Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky, MPSVR SR).</p>
4.8	Formal investigations	<p>Is there a licensing regime covering investigators?</p> <p>The Private Security Act defines procedures for conducting investigations and for providing supporting documentation to courts. A private security service operator is obliged to maintain all evidence relating to instructions from clients, contracts, visual communication records and physical surveillance records collected.</p> <p>Physical surveillance (overt or covert)</p> <p>Physical surveillance is covered by the Human Rights Convention and the Private Security Act.</p> <p>Electronic surveillance (e.g. tracking devices)</p> <p>See above.</p>

Visual and communication surveillance (using cameras, video or CCTV)

See above.

Communication intercept (including oral, written and electronic communication including bugging devices)

Any employer instigating procedures involving interception of communications must ensure that there is no infringement of Article 8 of the **European Convention on Human Rights** (i.e. that an individual's privacy is not violated).

The **Electronic Communications Act of 2011** ensures the 'privacy and protection of personal data processing in the sector of electronic communications'. This should be referred to when considering intercepting any communications, especially s. 55(3) which prohibits 'in particular tapping, listening, storage or other kinds of interception or surveillance of communications and the related data by persons other than users or without the consent of the users concerned, unless stipulated otherwise by this Act'.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

See above.

Formal interviews of staff

No specific restrictions apply to the use of formal interviews provided they adhere to human rights and data protection legislation.

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

See 'Communication intercept' (above).

Search and seizure of evidence, whether electronic or physical (overt or covert)

Employers have a general right to safeguard their own property used by employees. Investigators should have due regard to relevant health and safety legislation when carrying out search and seizure. It is advisable for employers to seek legal advice in specific circumstances.

Is it either usual or necessary to involve the police in investigations?

In cases of significant loss, companies usually contact the police and consequently the case is assigned to the civil/criminal court.

		<p>If the police are involved, at what stage in the investigation does this generally occur?</p> <p>The decision as to when and if to involve the police may depend on a number of factors such as the severity of the matter; the speed of response required (the police might not have adequate resources); access of the organisation itself to investigation capability (typically small organisations may be less able to respond to an incident than a large organisation with pre-defined resources and processes). The Penal Code requires reports of certain criminal acts to be made to the police.</p> <p>Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?</p> <p>Health and safety legislation requires an employer to keep records of any reportable injury, disease or dangerous occurrence (for example, injuries sustained in the course of a search of premises).</p> <p>What duties does the employer have to report information to local law enforcement authorities?</p> <p>The Anti-Money Laundering Act (see Section 4.1) imposes duties on persons working in the regulated sector to disclose any knowledge or suspicion of money laundering. Criminal penalties may be applied to those who fail to report suspicions.</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

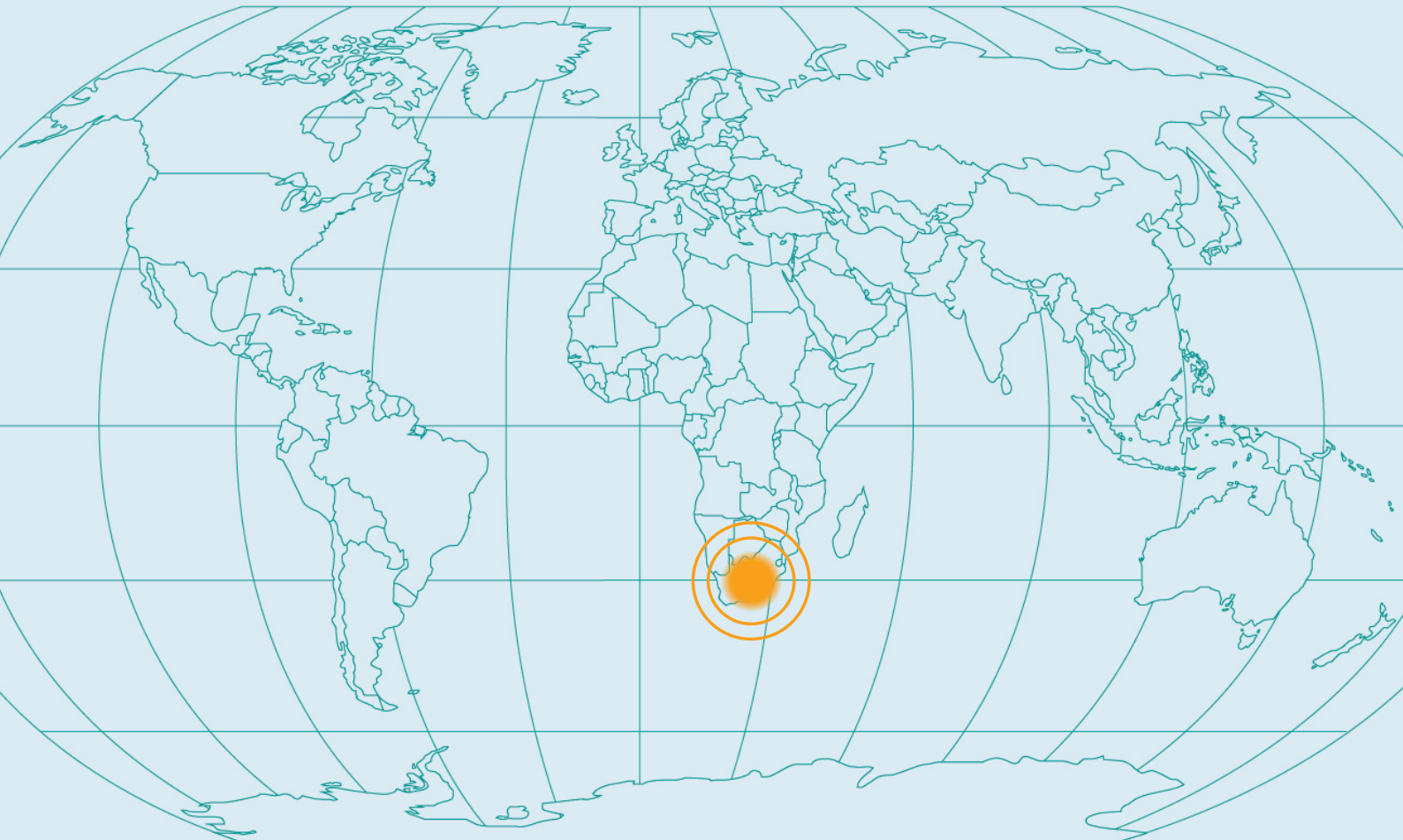
CPNI

Centre for the Protection
of National Infrastructure

SECURITY WATCHDOG
Part of Capita plc

South Africa

Personnel Security in Offshore Centres



● South Africa

- 1 Introduction
- 2 Personnel security measures during recruitment
 - 2.1 Culture of screening
 - 2.2 Major laws and regulations applying to pre-employment screening
- 3 Pre-employment checks
 - 3.1 Identity check
 - 3.2 Checks on eligibility to work
 - 3.3 Residency checks
 - 3.4 Criminal record checks
 - 3.5 Education checks
 - 3.6 Qualification checks
 - 3.7 Employment references
 - 3.8 Financial/credit checks
 - 3.9 Substance abuse screening
 - 3.10 Occupational health checks
- 4 Personnel security measures during employment
 - 4.1 Legal requirements
 - 4.2 Laws governing the rights of the employee or employer
 - 4.3 Local legislation that specifically governs the rights of the employer
 - 4.4 Local legislation that specifically governs the rights of the employee
 - 4.5 What avenues are open to employees who seek to challenge an employer's use of security procedures?
 - 4.6 What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?
 - 4.7 Availability of security measures
 - 4.8 Formal investigations

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

<p>1</p>	<p>Introduction</p>	<p>South Africa is becoming one of the most progressive countries in the global IT sector. Outsourcing in the region accounts for more than one-third of its IT services market.</p> <p>South Africa offers services to the domestic markets of Eastern Europe, Mexico, and Canada because of its proximity and affinity to their geography and culture. It is also compatible with Europe’s time zone.</p> <p>South Africa has strong skills in leadership, customer service, human resource, operations, and technical resource management. Its BPO sectors are highly involved in telecommunications, insurance, financial services, and other outsourced processes that involve Web design and development, sales services, human resources, data capture and conversion, benefits administration, and accounting. South Africa also has financial acumen in loan processing and collection, mortgages and insurance.</p> <p>Security screening of employees is undertaken regularly by companies in South Africa at both the pre-employment and post-employment stages. There is a developed legal framework governing the rights of employees and employers, including constitutional rights and specific laws governing rights of access to information, investigations and reporting of security concerns, amongst other things. Employee security measures are widely available to employers in South Africa. The guiding principal under the South African Constitution is that actions should be balanced and proportionate to the threat.</p> <p>There are a range of sources of public information available to verify the background of employees in South Africa, including voters’ roll information and access to a number of commercial credit bureaux. Investigations may generally be undertaken by an employer (for example, in situations where security concerns arise). Employee screening operations and investigations work may be outsourced to third parties in South Africa, and there is a licensing regime covering the private security industry.</p>
<p>2 Personnel security measures during recruitment</p>		
<p>2.1</p>	<p>Culture of screening</p>	<p>In South Africa, a number of sectors (notably regulated functions such as those in the financial services industry, licensed functions, security and government) have adopted pre-employment screening procedures. This is often conducted through specialised background screening companies.</p> <p>The level of pre-employment screening is generally commensurate with the role and responsibilities of the individual concerned. For example, an individual with access to sensitive financial data would generally be subject to higher levels of screening than one who did not have such access. The level of screening is at the discretion of the employer.</p> <p>In the public sector, specific government agencies, for example the Financial Intelligence Centre and Intelligence Services, conduct detailed pre-employment screening on their employees as required by legislation. The main legislation includes:</p>

		<ul style="list-style-type: none"> • the Financial Intelligence Centre Act 38 of 2001 • the Intelligence Services Act 38 of 1994 and • the Public Service Act 102 of 1994. <p>Under the Immigration Act an employer must ensure that a prospective employee has the right to work in the country. Employers who employ individuals who do not have the right to work in South Africa are liable to criminal prosecution.</p>
2.2	Major laws and regulations applying to pre-employment screening	<p>The principal legislation governing employee screening is:</p> <ul style="list-style-type: none"> • the Basic Conditions of Employment Act 75 of 1997 (amended 2013), which regulates fair labour practices referred to in s. 23(1) of the Constitution and includes matters such as occupational accidents, informing employees of their rights, termination of employment, investigations, enforcement and legal proceedings • the Employment Equity Act 55 of 1998 (amended 2013), which covers issues such as unfair discrimination, medical testing, psychometric testing and certain trade union activities and • the Labour Relations Act 66 of 1995 (amended 2002), which provides procedures for the resolution of labour disputes through statutory conciliation, mediation and arbitration. <p>There are regulatory requirements in relation to ‘fit and proper’ tests, in particular those regulated by the Financial Services Board. The major laws and regulations applying to pre-employment screening in South Africa include:</p> <ul style="list-style-type: none"> • the National Credit Act No. 34 of 2005, which regulates the use of credit information to promote a fair and non-discriminatory marketplace for access to consumer credit • the Constitution of the Republic of South Africa, and • the Promotion of Access to Information Act No. 2 of 2000 (amended 2002), which governs the right of access to records of both public and private bodies. <p>A change to the Immigration Act was due to be announced sometime in 2014 amending the procedures and rules for work permits/visas. It is anticipated that this will adversely affect some foreign nationals working in South Africa, owing to changes in immigration categories and criteria. Further information was not available at the time of writing.</p> <p>Complete Acts together with any amendments can be searched for at www.gov.za/documents/index.php.</p>

3	Pre-employment checks	
3.1	Identity check	<p>It is common to undertake checks on attributed identity (given name, date of birth, addresses).</p> <p>In case of lost or stolen identification documentation, certain employers would require the employee to provide an affidavit or a copy of a report to the South African Police Services, or to apply to the Department of Home Affairs for a new Identity Document.</p> <p>Forms of verification include a green, barcoded Identity Document (a booklet that is similar to a passport and is issued by the South African Department of Home Affairs). This was the official form of national identification specified by the Identification Act 68 of 1997 but an amendment has introduced micro-chipped identity cards that are being phased in from July 2013 for new applicants and renewals.</p>
		<p>Other forms of identification are still required, for example by financial institutions in exceptional circumstances. The green, barcoded Identity Document and the new replacement cards are issued to South African citizens and not residents. An individual may apply for a South African ID if he or she is a South African citizen or permanent resident over 16 years of age.</p> <p>The official ID document is the only accepted proof of ID that enables eligible voters to register to vote (an individual may apply for a Temporary Identification Certificate subject to verification of the applicant's fingerprints); alternatively, a passport or photocard drivers' licence. Marriage, birth or adoption certificates offer a lower level of identity verification.</p> <p>The holder of the ID must physically present it to the employer who will check the holder's name against available databases (for example the voters' roll or a credit bureau database). The credit bureaux charge a fee for verifying information.</p>
3.2	Checks on eligibility to work	<p>Such checks are required if the individual is not a national of South Africa.</p> <p>Generally, employers would ask prospective employees to provide work permit/visa documentation. The Department of Home Affairs can be contacted for details on how to obtain a work permit. See www.home-affairs.gov.za for further details.</p> <p>A change to the Immigration Act was due to be announced sometime in 2014 amending the procedures and rules for work permits/visas. It is anticipated that this will adversely affect some foreign nationals working in South Africa, owing to changes in immigration categories and criteria. Further information was not available at the time of writing.</p> <p>The employer can also contact the Department of Home Affairs or use a background screening agency to perform work permit and nationality checks.</p>

<p>3.3</p>	<p>Residency checks</p>	<p>It is common practice in South Africa to undertake checks on both current and former addresses.</p> <p>Residency information is generally accessed by the employer or a third party acting on its behalf. Items checked may include:</p> <ul style="list-style-type: none"> • voters' roll • bank statements • telephone accounts • retail accounts • the telephone directory and • utility accounts. <p>The voters' roll can be accessed through the local Municipal Electoral Office (www.elections.org.za/content/Voters-Roll/About-the-Voters-Roll/). There is no fee for this. Credit bureaux may be used to confirm voter information, although their data is usually obtained from credit references. At the last census, in October 2011, the total population of South Africa was around 51 million. Registration statistics in 2014 suggested that around 25 million individuals were registered to vote. The voters' roll must be searched by national ID number.</p> <p>Credit bureaux can also conduct these checks for a fee. The main credit bureaux in South Africa are Transunion (www.transunion.co.za) and Experian (www.experian.co.za). Both require subscription to their services. Costs for subscriptions vary with the type of subscription.</p>
<p>3.4</p>	<p>Criminal record checks</p>	<p>Name of certificate</p> <p>Police Clearance Certificate (PCC).</p> <p>Department that holds records</p> <p>South African Police Service (SAPS).</p> <p>Where to apply within country</p> <p>The Head of the South African Criminal Record and Crime Scene Management, (For attention: Police Clearance Certificates), Bothongo Plaza West, CRC Client Service Centre, 1st Floor, Room 14, 271 Frances Baard Street, Pretoria, South Africa.</p> <p>Telephone: +27 (0)12 393 3928 Fax: +27 (0)12 393 3909 Email: crc-nameclear@saps.org.za crc.clientserv.sec@saps.org.za crc.client@saps.org.za</p> <p>Website: http://www.saps.gov.za/services/applying_clearance_certificate.php</p>

	<p><i>In person</i></p> <p>A list of regional police stations can be found at www.saps.gov.za/.</p> <p><i>By post</i></p> <p>The Head of the South African Criminal Record and Crime Scene Management, (For attention: Police Clearance Certificates), Private Bag X308, Pretoria, Gauteng, South Africa, 0001.</p>
	<p>How to apply within country</p> <p><i>In person</i></p> <p>The individual can apply at any of the police stations or the main address. He or she needs to provide a full set of fingerprints (can be taken at a local police station); full name, surname, date of birth, place of birth and identity number (if available) must be recorded on the fingerprint form. Original ID must be provided if the certificate is requested in person.</p> <p>There is no specific application form but the following information must be provided:</p> <ul style="list-style-type: none"> • surname • maiden name (proof should be provided if the applicant would like the maiden name to appear on the certificate) • forenames • date of birth • place of birth • South African ID number (if applicable) • date • signature • mailing address in the country of application • Zip/postal code • telephone/mobile phone number (if the mobile number is South African, update texts will be sent) and • specify how the results should be issued, i.e. by courier, post or counter collection, etc; if they are to be sent by post, include a fee to cover this or a stamped self-addressed envelope.

		<p><i>By post</i></p> <p>The individual must submit the same information as listed in the ‘In person’ section above and send it to the ‘By post’ address above. A copy of the individual’s ID and proof of payment must be included.</p> <p>The individual can track the application on the SAPS website by using the link to the SAPS website and clicking on ‘behaviour certificate’.</p> <p>Who can apply</p> <p>Individuals over the age of 14 years or third parties (with the individual’s consent).</p> <p>Cost</p> <p>R59.00 by bank guaranteed cheque, banker’s draft or electronic payment into the South Africa Police Service account:</p> <ul style="list-style-type: none"> • ABSA cheque account number 4054522787 • Branch code 632005 • SWIFT code ABSA ZAJJ and • made payable to the National Commissioner of the South African Police Service. <p>For electronic payment, the letters ‘PCC’ must be added together with the initials and surname of the applicant.</p> <p>Turnaround</p> <p>Within 14 working days from receipt of the application at the Criminal Record Centre, but where previous convictions are identified, the processing time is longer and there is no fast-track service available.</p> <p>Further information can be obtained from the CPNI guidance on <i>Overseas Criminal Record Checks</i> which can be found at www.cpni.gov.uk/advice/Personnel-security1/Overseas-criminal-record-checks/.</p>
3.5	Education checks	<p>Education checks are often required by employers to establish that a prospective employee has attended the educational establishments claimed.</p> <p>Typical information provided is dates of joining and leaving the educational institution (school, college, university), subject of study, courses and degree(s) and final mark. In many cases this information will only be confirmed and not volunteered. Any information deemed to be private is not accessible.</p> <p>Often questions regarding the character of an individual will not be answered by educational institutions in writing, although in some cases a verbal character reference might be obtained from a tutor or professor who knows the individual.</p> <p>Verification may be requested directly from the educational establishment. Applications must typically be made in writing and provide all known information, e.g. full name, date of birth, subject of study. Many organisations have standard processes for dealing with reference enquiries. The consent of the individual is generally required.</p>

		<p>Results of education checks should be provided on headed paper. This ensures that the issuing institution will have some liability for ensuring that the data is correct and reliable.</p> <p>Where the educational establishment is not well known, it may be necessary to undertake additional checks to verify its authenticity. In particular, employers should be alert to the risk of fake establishments and/or fake qualifications issued by such establishments.</p> <p>The National Credit Act 34 of 2005 states that credit checks can be conducted to verify educational qualifications and employment, although the consent of the individual must be obtained before conducting this check as s. 14 of the Constitution of the RSA, 1996 guarantees a person's right to privacy. The Electronic Communications and Transactions Act 25 of 2002 deals with the protection of personal information, albeit on a voluntary basis.</p>
3.6	Qualification checks	<p>Verification of qualifications (academic or professional) is a regular part of pre-employment screening in South Africa.</p> <p>Typical information provided is dates of joining and leaving the educational institution or professional body, membership status (professional body), status and type of qualification. In many cases, all known information has to be provided. The institution will confirm this information, though it will not volunteer any data.</p> <p>Generally, questions regarding the character of an individual will not be answered by educational institutions in writing, although in some cases a verbal character reference might be obtained from a tutor or professor who knows the individual.</p> <p>Verification of qualifications is generally undertaken directly with the establishment concerned. Similar considerations exist as for education checks (see Section 3.5). In qualification checks, usually only the information provided by the employer is verified. Seeking to obtain other information may be regarded as an invasion of personal privacy.</p>
3.7	Employment references	<p>Employment references are commonly taken up in South Africa. The consent of the individual is generally required to undertake these checks.</p> <p>Many employers have adopted policies that prohibit the provision of character references and comments on performance, written or verbal. Most employers will not provide information on salaries, sickness records or parental leave.</p> <p>Verification is undertaken directly with the respective employer. Where the identity of a previous employer is in doubt, further investigation may be required to verify its existence/background. Such checks are generally performed at the discretion of the employer and will depend on company policy.</p>

		<p>The Constitution of the RSA, 1996 prohibits discrimination based on character references. The Employment Equity Act 55 of 1998 (amended 2014) states in s. 6(1) (prohibition of unfair discrimination): ‘No person may unfairly discriminate, directly or indirectly, against an employee, in any employment policy or practice, on one or more grounds, including race, gender, sex, pregnancy, marital status, family responsibility, ethnic or social origin, colour, sexual orientation, age, disability, religion, HIV status, conscience, belief, political opinion, culture, language, birth or on any other arbitrary ground.’</p> <p>It is therefore common practice that this type of information is not requested when checking references. Character references are provided at the discretion of the employer and are not always given. They may only offer verification of basic employment history and reason(s) for leaving. These are generally performed at the discretion of the employer.</p>
<p>3.8</p>	<p>Financial/ credit checks</p>	<p>Generally, employers are prohibited by legislation from conducting financial or credit checks on employees. However, if an employee is being considered for a position that requires trust and honesty or the handling of cash or finances, credit checks can be carried out. Explicit consent must be obtained from the prospective employee.</p> <p>In South Africa credit checks are governed by the National Credit Act 34 of 2005 (see Section 2.2). Although not specifically relevant to character references, the Act stipulates that ‘consumer credit information relating to the following subjects may not be contained on the records of the credit bureau:</p> <ul style="list-style-type: none"> • race • political affiliation • medical status or history • religion or thought, belief or opinion • sexual orientation, except to the extent that such information is self-evident from the [person]’s marital status and list of family members or • membership of a trade union, except to the extent that such information is self-evident from the record of the [person]’s employment information.’ <p>A number of credit information bureaux provide credit data. Well-known providers include Experian and Transunion. These records can be accessed online by employers, who must be registered with the information provider. Costs depend on the provider and the subscription type. Requests for credit information will leave a record on the individual’s credit file.</p> <p>Credit records can be subject to error or omission. Individuals can apply to the credit bureau concerned to have their record amended if they believe it to be inaccurate. All credit bureaux have established appeals processes.</p>

3.9	Substance abuse screening	<p>Substance abuse screening may be undertaken in South Africa. It is governed by the Constitution of RSA, 1996 which guarantees the individual's right to privacy in s. 14.</p> <p>The Employment Equity Act 55 of 1998 states in s. 7 (medical testing) that medical testing of an employee is prohibited, unless legislation permits or requires it, or it is justifiable in the light of medical facts, employment conditions, social policy, the fair distribution of employee benefits or the inherent requirements of a job. Testing of an employee to determine HIV status is prohibited unless such testing is determined justifiable by the Labour Court under s. 50(4) of the Employment Equity Act.</p>
3.10	Occupational health checks	<p>See Section 3.9.</p> <p>Occupational health checks are subject to the rights of privacy outlined in s. 14 of the Constitution of the RSA, 1996.</p>
4 Personnel security measures during employment		
4.1	Legal requirements	<p>A number of laws govern the application of employment security procedures in South Africa. The key laws are summarised below. Employers should seek legal advice in specific circumstances if in doubt.</p> <p>Constitution of the Republic of South Africa 1996:</p> <ul style="list-style-type: none"> • Section 9 prohibits unfair discrimination on one or more grounds, including race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth. • Section 14 grants everyone the right to privacy, which includes the right not to have the privacy of their communications infringed. • Section 23 The grants everyone the right to fair labour practices. National legislation may recognise union security arrangements contained in collective agreements. Any limitation these arrangements must comply with s. 36(1). • The Electronic Communications and Transactions Act 25 of 2002 regulates the protection of personal information. • The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 regulates the interception of certain information. • The Protection of Information Act 84 of 1982 (amended 2010) regulates the prohibition of secret state information. • The Protected Disclosures Act 26 of 2000 (Whistleblower Act) outlines which employees in both the private and the public sector may disclose information regarding unlawful or irregular conduct by their employers or other employees of their employers and protects employees who make a disclosure that is protected under the Act.

		<ul style="list-style-type: none"> • The Promotion of Access to Information Act 2 of 2000 covers the constitutional right of access to any information held by the state or by another person and that is required for the exercise or protection of any rights, and connected matters. • Various trade unions exist in South Africa. The Labour Relations Act 66 of 1995 gives effect to s. 27 of the Constitution and regulates the organisational rights of trade unions. <p>Complete Acts together with any amendments can be searched for at www.gov.za/documents/index.php.</p> <p>Mandatory anti-fraud measures in South Africa</p> <p>Specific legislation in South Africa covers the requirement to report suspicious, unusual or corrupt activities. This includes anti-money laundering legislation. The key legislative instruments are:</p> <ul style="list-style-type: none"> • Financial Intelligence Centre Act 38 of 2001 (FICA) • Protection of Constitutional Democracy against Terrorist Related Activities Act (POCDATARA) 33 of 2004 • Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA) and • Prevention of Organised Crime Act No. 121 of 1998 (POCA). <p>Complete Acts together with any amendments can be searched for at http://www.gov.za/documents/index.php.</p>
4.2	Laws governing the rights of the employee or employer	
4.3	Local legislation that specifically governs the rights of the employer	The employer may be protected by intellectual property rights (including defamation, slander and trademark law), and rights imposed under the employment contract. Legal action for breach of contract may restrain an employee from dealing in client-confidential information although it is unlikely to deter more serious offences without the imposition of other controls (such as physical access or monitoring controls, as described below).
4.4	Local legislation that specifically governs the rights of the employee	As detailed above, there is legislation that governs the rights of an employee (and third parties). Whilst this may restrict the level of investigations permissible, the guiding principle under the Constitution is that any response should be balanced and proportionate to the threat.
4.5	What avenues are open to employees who seek to challenge an employer's use of security procedures?	Individuals may bring claims against their employer under the legislation set out above. Additionally, many employers have established complaints procedures, which may involve local trade union representatives to represent the employee.

<p>4.6</p>	<p>What avenues are open to employees who seek to challenge their dismissal which was based on the results of an organisation's security procedures?</p>	<p>A claim for unfair dismissal may be brought under the Basic Conditions of Employment Act. The claim may be upheld by an employment tribunal if it is determined that the actions of the employer breached the employees' rights at law. Under the Protected Disclosures Act employees who make a 'protected disclosure' via such as a whistleblowing hotline may be protected from dismissal.</p> <p>The Labour Relations Act 66 of 1995 Schedule 8, 'Code of Good Practice: Dismissal' regulates the disciplinary process. Section 3 states:</p> <p>(1) 'All employers should adopt disciplinary rules that establish the standard of conduct required of their employees. The form and content of disciplinary rules will obviously vary according to the size and nature of the employer's business. In general, a larger business will require a more formal approach to discipline. An employer's rules must create certainty and consistency in the application of discipline. This requires that the standards of conduct are clear and made available to employees in a manner that is easily understood. Some rules or standards may be so well established and known that it is not necessary to communicate them.</p> <p>(2) The courts have endorsed the concept of corrective or progressive discipline. This approach regards the purpose of discipline as a means for employees to know and understand what standards are required of them. Efforts should be made to correct employees' behaviour through a system of graduated disciplinary measures such as counselling and warnings.</p> <p>(3) Formal procedures do not have to be invoked every time a rule is broken or a standard is not met. Informal advice and correction is the best and most effective way for an employer to deal with minor violations of work discipline. Repeated misconduct will warrant warnings, which themselves may be graded according to degrees of severity. More serious infringements or repeated misconduct may call for a final warning, or other action short of dismissal. Dismissal should be reserved for cases of serious misconduct or repeated offences.'</p>
<p>4.7</p>	<p>Availability of security measures</p>	<p>Restriction of access to premises</p> <p>Generally there is no legal restriction on restricting access to premises.</p> <p>Restriction of access to certain rooms/zones on the premises</p> <p>Certain legislation regulates access to premises, rooms or zones. This includes, but is not limited to:</p> <ul style="list-style-type: none"> • the Mine Health and Safety Act 29 of 1996 – a mining company must ensure that trespassers cannot have easy access to their property/ operations (for health and safety reasons) • the Occupational Health and Safety Act 85 of 1993 – a company must ensure that the health and safety of persons other than employees are not endangered • the National Key Points Act 102 of 1980 – the owner of a key point must take reasonable steps to ensure the protection of that point and

- the Protection of Information Act 84 of 1982 protects certain state security information. It refers to prohibited places. Persons who enter such places could be guilty of committing a criminal offence.

Physical screening (on entry/exit)

No specific legislation governs the use of physical screening measures by employers. Their use may be generally subject to the Constitution.

Prohibition of removal of data from the premises (hard-copy)

Certain legislation governs the protection of data in South Africa. This includes the Protection of Information Act 84 of 1982.

Prohibition of removal of data from the premises (electronic)

Certain legislation governs the protection of data in South Africa. This includes the Electronic Communications and Transactions Act 25 of 2002.

Visual surveillance (CCTV or other cameras), either overt or covert

This is not regulated by specific legislation. It is common practice to use CCTV or similar systems to monitor employee activity.

The **Regulation of Interception of Communications Act (RICA)** governs legal surveillance in South Africa. IT falls within 'indirect communication' under the Act. (See under 'Overt/covert monitoring of internal or external communications' below and also RICA s. 2(6)(1)c and s. 2(6)(2)c and d).

Overt monitoring of access to IT and other equipment

See above.

Covert monitoring of access to IT and other equipment

See above.

Reporting hotlines (anonymous)

The use of whistleblowing hotlines is widespread in South Africa. It is governed by the Whistleblower Act. The Act details which types of information may be disclosed, and to whom they may be disclosed, in order for the employee to qualify for protection under the Act.

In practice, anonymous disclosures may be less welcome than confidential reports, as they are hard to corroborate, difficult to investigate and often impossible to remedy. As such, setting up and publicising a hotline through which the public and employees can anonymously report suspected wrongdoing may not be good practice when attempting to promote and encourage a culture of openness and transparency.

Reporting hotlines (confidential)

Section 6(2) of the Whistleblower Act makes provision for confidential hotlines. Some companies encourage the use of such hotlines by employees. Section 6(2) of the Act reads: 'Any employee who, in accordance with a procedure authorised by his or her employer, makes a disclosure to a person other than his or her employer is deemed, for the purpose of the Act, to be making the disclosure to his or her employer'.

Use of alerts/automated warning systems to identify unusual employee behaviour (out of hours activities, duplicate payments)

It is common practice in South Africa to use alerts, automated warning systems and exception reports. Their use is subject to s. 14 of the Constitution as it relates to privacy and to the Communication-Related Information Act 70 of 2002 which prohibits the interception of communications and outlines exceptions.

Overt or covert monitoring of internal or external communications (telephones, mail, email or internet)

The Electronic Communications and Transactions Act 22 of 2002, Chapter VIII, 'Protection of Personal Information' applies only to personal information that has been obtained through electronic transactions. Section 51 specifies the principles for collecting personal information electronically, which require a data controller to:

- have written permission from the data subject for the collection, collation, processing or disclosure of that subject's personal information unless permitted or required to do so by law. If data is deemed to be critical data by the Minister, disclosure is required (via a register kept by the Department) to investigating officers, national security agencies, cyber inspectors and civil proceedings, and health records in terms of the Promotion of Access to Information Act. In practice the interpretation of this clause is very broad and a court may allow avoidance if it deems this necessary.
- not electronically request, collect, collate, process or store personal information not needed for the purpose for which the personal information is required.
- disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.
- not use the personal information for any purpose other than the disclosed purpose without written permission from the data subject, unless permitted or required to do so by law.
- for as long as the personal information is used and for at least one year after, keep a record of the personal information and the specific purpose for which it was collected.
- not disclose any personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.
- for as long as the personal information is used and for at least one year after, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.
- delete or destroy all personal information that has become obsolete.

A party controlling personal information may use that information to compile statistical profiles and may freely trade with such profiles and statistical data, as long as these cannot be linked to any specific data subject by a third party.

		<p>Can employers require employees (a) to inform them of changes in circumstances, e.g. change of address, marital status and financial circumstances etc or (b) use line management structures to enhance security, e.g. by asking line managers to complete an annual security appraisal of staff?</p> <p>Generally this step is available to employers in South Africa, although employers would not be legally entitled to ask questions concerning marital status and financial status. However, there are exceptions under the National Credit Act 34 of 2005 which states that employers can obtain financial information from a credit bureau:</p> <ul style="list-style-type: none"> • to investigate fraud, corruption or theft, provided that the SAPS or any other statutory enforcement agency conducts the investigation • to detect and prevent fraud • when considering a candidate for employment in a position that requires trust and honesty and entails the handling of cash or finances • when assessing the debtors book of a business for the purposes of: <ul style="list-style-type: none"> – sale of the business or debtors book – determining the value of the business or debtors book – setting a limit on provision of any continuous service – assessing an application for insurance – verifying educational qualifications and employment – obtaining consumer information to distribute unclaimed funds, including pension funds and insurance claims and – developing a credit scoring system by a credit provider or credit bureau. <p>For all of these checks, the explicit consent of the employee must be obtained.</p> <p>Annual security appraisals are not generally performed by companies in South Africa.</p>
<p>4.8</p>	<p>Formal investigations</p>	<p>Is there a licensing regime covering investigators?</p> <p>Various laws relate directly to the performance of security officers in South Africa. The main legislation is the act establishing the Private Security Industry Regulatory Authority (PSIRA) and the accompanying Private Security Industry Regulations, 2002. Under this act all private investigators are required to register with PSIRA. Persons or companies that offer investigation services but attempt to conceal these activities under other titles are covered by the legislation. The Act specifically excludes non-citizens and non-residents (and certain categories of citizens and residents) with penalties of up to two years in jail for the offender if prosecuted. This legislation also makes it an offence to employ an unregistered person and company, meaning that the client can also be prosecuted.</p> <p>For further information, see www.psira.co.za</p>

Physical surveillance (overt or covert)

The law governing surveillance in South Africa is the RICA as detailed in **Section 4.1**.

Grounds for surveillance orders are specified in Chapter 3 of RICA, and include criminal investigations of serious offences; gathering information regarding actual or potential threats to public health and safety and national security or actual threats to other compelling national economic interests; gathering information concerning property that could be used in a serious offence or the proceeds of unlawful activities and to assist foreign law enforcement agencies in matters regarding organised crime or terrorism under a mutual assistance agreement.

While 'serious offence' is defined (some examples include high treason, terrorism, sabotage, sedition, threat of risk to life, offences related to drugs/trafficking, corruption, smuggling ammunition, firearms, explosives and unlawful possession, possession of endangered, scarce or protected game, plants, illicit dealing in precious metals or stones, offences relating to the Prevention of Organised Crime Act, any offence for which seven or ten years' imprisonment is the penalty), there is still no definition or qualification of the 'national interest', or when it may be compelling. The threshold of 'reasonable grounds to believe' remains the standard for a Judge to grant an order, but further grounds that need to be satisfied have been built in an attempt to enhance this weak standard.

Section 6 makes specific provision for a business to intercept business-based communications for the integrity of its operations. A business may have a right to intercept all workplace-based communications, but it is highly advisable to do so only when the business:

- has devised and implemented a clear and appropriate acceptable use policy (AUP) that is not excessively invasive or burdening
- communicates its AUP to all employees regularly and uniformly
- only intercepts communications that are clearly private when there is sufficient good cause to suspect that the business's interests are being compromised, and there is a legitimate expectation that evidence of such compromise is to be found in those communications and
- applies the provisions of the AUP consistently.

Electronic surveillance (e.g. tracking devices)

See 'Physical surveillance' above.

Visual and communication surveillance (using cameras, video or CCTV)

See 'Physical surveillance' above.

Communication intercept (including oral, written and electronic communication including bugging devices)

Communication intercept is governed by RICA. RICA introduced a general prohibition of communication interception, subject to certain stipulated exceptions; contravening its provisions without lawful excuse constitutes an offence that may result in penalties of up to R2million, or imprisonment for up to ten years

'Intercept' is defined by RICA as the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes:

- the monitoring of any such communication by means of a monitoring device
- viewing, examination or inspection of the contents of any indirect communication and
- diversion of any indirect communication from its intended destination to any other destination, and 'interception' has a corresponding meaning.

Corporate email systems and phone lines used by an employee fall under RICA and 'monitoring' and 'intercept' are interchangeable for the purposes of its application.

The three instances in which a workplace-based interception is lawful are:

- where the intercepting party is a party to the communication being intercepted
- where one of the parties to the communication has provided prior written consent to the interception and
- where the intercepting party is the business and the communication takes place in carrying on that business – the so-called business exception.

Section 6(1) of RICA provides that any person may, in the course of carrying on any business, intercept any indirect communication:

- by means of which a transaction is entered into in the course of that business
- which otherwise relates to that business or
- which otherwise takes place in the course of carrying on that business in the course of its transmission over a telecommunication system.

The section goes further and also requires the express or implied consent of the system controller. The monitoring or keeping of records by an employer must be done for a legitimate purpose, namely:

- to establish the existence of facts
- to investigate or detect the unauthorised use of the employer's telecommunication system or
- to secure the effective operation of that system.

In addition to the above, the telecommunication system concerned must be provided for use wholly or partly in connection with that business; the system controller must have made all reasonable efforts to inform individuals using the telecommunication system in advance that indirect communications transmitted through it may be intercepted, and the system controller must intercept the communication itself or have consented to such interception.

It is important to note that the business exception only applies to an indirect communication that is transmitted over a telecommunication system, as defined in the Telecommunications Act, which is intercepted during the course of transmission. It is also important to note that RICA requires that the indirect communication be intercepted during the course of transmission. Thus, where a message has already arrived at its destination, the business exception no longer applies.

Since there are a variety of communications that fall outside the business exception, employers should obtain written consent from both their current and future employees in order to allow them to lawfully intercept communications in circumstances where the business exception does not apply.

An employee's emails and internet usage may be lawfully intercepted by his or her employer provided all the requirements listed above have been complied with.

Computer or database surveillance (using either hardware or software tools, including forensic tools)

See 'Physical surveillance' above.

Formal interviews of staff

Key legislation governing formal interviews of staff includes the **Civil Proceedings Evidence Act No 25** of 1965. The Act does not prevent an employer from undertaking formal interviews although it is advisable that such interviews are conducted in accordance with it. The Act should be taken into account when considering the admissibility of evidence (ss 33–38 deal with miscellaneous provisions relating to documentary evidence).

Transactional surveillance (including phone logs, electronic mail logs, website activity logs, credit card activity, building access logs, credit card activity, computer access logs and financial transactional data)

See 'Physical surveillance' above.

Search and seizure of evidence, whether electronic or physical (overt or covert)

See 'Physical surveillance' above.

Is it either usual or necessary to involve the police in investigations?

There is no requirement to involve the police in investigations although this may be preferable where criminal proceedings are contemplated.

If the police are involved, at what stage in the investigation does this generally occur?

The police may or may not be involved in an investigation. The decision as to when and if to involve the police may depend on a number of factors such as the severity of the matter; the speed of response required (the police might not have adequate resources); access of the organisation itself to investigative capability (typically, small organisations may be less able to respond to an incident than a large organisation with pre-defined resources and processes).

Are there any practical considerations to be aware of when involving the police/law-enforcement authorities?

In South Africa the police have limited resources and therefore cannot realistically investigate all cases in detail. An organisation may undertake its own investigation, alone or in conjunction with a third party. Where an investigation is likely to progress to a criminal complaint, it is essential that the investigation is conducted to the standards required for a criminal case. This includes the gathering of physical and electronic evidence. Information that is not gathered to an adequate evidential standard may be inadmissible in court. The police may be dissuaded from taking on a case unless they can be certain that information has been gathered to adequate evidential standards, or they have been involved from the outset. A key legislative consideration is the Criminal Procedure Act No. 51 of 1977.

What duties does the employer have to report information to local law enforcement authorities?

The PRECCA imposes duties on the employer to report information to law enforcement authorities. Section 34 places a duty to report corrupt transactions:

' (1) Any person who holds a position of authority and who knows or ought reasonably to have known or suspected that any other person has committed

		<p>(a) an offence under Part 1, 2, 3 or 4, or section 20 or 21 (in so far as it relates to the aforementioned offences) of Chapter 2; or</p> <p>(b) the offence of theft, fraud, extortion, forgery or uttering a forged document, involving an amount of R100,000 or more, must report such knowledge or suspicion or cause such knowledge or suspicion to be reported to any police official.</p> <p>(2) Subject to the provisions of section 37 (2), any person who fails to comply with subsection (1), is guilty of an offence.'</p>
	<p>Sources</p>	<p>Open Source Government and Legal Repositories</p> <p>CPNI Guidance Documents</p>

Published by Security Watchdog, part of Capita plc on behalf of the **Centre of the Protection of National Infrastructure (CPNI)**. Security Watchdog is the international industry leader and subject matter expert in all areas of background screening. Security Watchdog undertakes best practice pre and post-employment screening to underpin informed recruitment decisions. Screening is carried out with candidate consent in compliance with data protection regulations. Security Watchdog is a leading provider of risk mitigation solutions in EMEA and internationally and works with over 10% of FTSE 100 companies. More information can be found at www.securitywatchdog.org.uk

© Crown Copyright 2014

The text of this publication may not be reproduced, nor may talks or lectures based on material contained within the document be given, without written consent from the Centre for the Protection of National Infrastructure (CPNI).