CPNI
Centre for the Protection of National Infrastructure

大成 DENTONS

New and emerging technologies
Key considerations

Collaborative communication channels (E.g. WhatsApp, Slack, Flock, Google Hangouts)

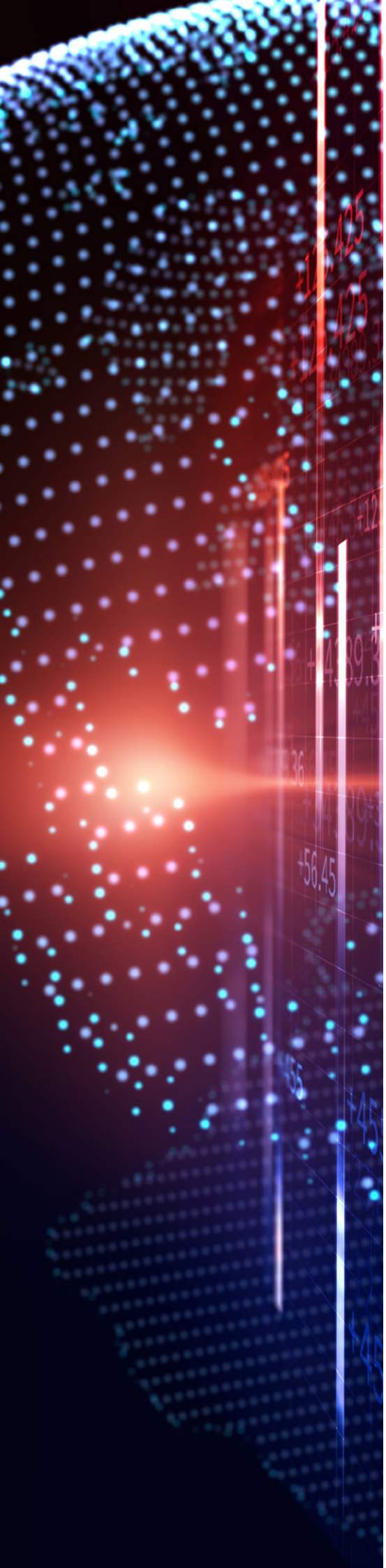
- Employers should adopt clear policies, applied rigorously and consistently that only permitted work equipment or devices (which can be the subject of monitoring) can be used for work purposes and for the exchange of work-related information. The policies should be written in broad terms to cover new forms of communication channels which may emerge.

Bring your own device (BYOD)

- See also UK Fraud Advisory Panel's guidance on BYOD policies, and the ICO BYOD guidance.
- Key considerations for the employer as data controller include:
  - what type of data is held;
  - where the data may be stored (on the device, on a company server, or elsewhere);
  - how it is transferred;
  - potential for data leakage;
  - blurring of personal and business use;
  - the device's security capabilities;
  - what to do if/when the person who owns the device leaves employment; and
  - how to deal with the loss, theft, failure and support of a device.
- Every employer should have an effective BYOD policy in place which sets clear rules and responsibilities. Policies should be backed up by appropriate training and refreshers for all staff, so that awareness is maintained.
- Monitoring should remain transparent, proportionate and not excessive, especially in relation to periods of personal use. It is important to keep monitoring to the specified purpose and not, for example, used for ongoing surveillance or monitoring of users. It must comply with the restrictions within existing data protection law.
- Use Legitimate Interests Assessments (LIAs) to weigh the interests of the organisation against the impact on personal privacy.

Big data, artificial intelligence (AI) and machine learning

- Such processing should be fair, transparent and proportionate. This relates to any personal data being used and any that may be generated by such a system.



- Individuals have a right in the UK under the GDPR to not be subject to a decision based solely on automated processing, including profiling, which significantly affects an individual, e.g. E-recruitment decisions being made without human intervention. Consider this right when using user behaviour analytics (or 'black box') solutions to assess employees' IT systems activity and ensure there is some human review before employees are likely to be impacted.
- In terms of balancing privacy and business interests, questions of the sensitivity of such analytics might arise and the level of false positives that might be generated (and subsequently investigated, thus exposing analysts to personal data unnecessarily).
- Personal data must be accurate. Within data analytics, even if the data is reported accurately (something which isn't always true in itself), this does not necessarily mean the inferences or conclusions drawn from it are accurate. Consider carefully these conclusions to ensure that more intrusive monitoring (which may be the next step in your process) is necessary, and that there are no less invasive methods which may be used to mitigate the potential threat identified.
- Note the right of individuals to seek access to the personal data held on them, including that obtained from such analytics.
- Consider Data Protection Impact Assessments (particularly involving new technologies and sensitive personal data processing) which are required under GDPR in the UK. Incorporate privacy by design and by default.

Biometric monitoring

- Consider implications from new biometric technologies which may form part of a monitoring programme. E.g. an employer using AI to analyse voice waves of its employees to detect any concerns (e.g. from voice tone).
- Biometrics are 'special category' data under GDPR and can only be processed in very limited circumstances. Consider less intrusive ways of monitoring (e.g. other system logs).

Social media analysis

- Be careful of unconscious bias during the recruitment process when looking at social media profiles and comments. An unsuccessful candidate may argue they were not offered a role due to a protected characteristic found on their social media profiles or posts, which would not have been apparent to the employer had they not accessed that content (in breach of the Equality Act 2010).
- Candidates for employment are required to be expressly told of any social media vetting that will be carried out and vetting should only be used as a means of obtaining specific information, not as a means of general intelligence gathering.
- Social media vetting should only be carried where there are particular and significant risks to the employer, customers or others and where there is no reasonably practicable alternative.

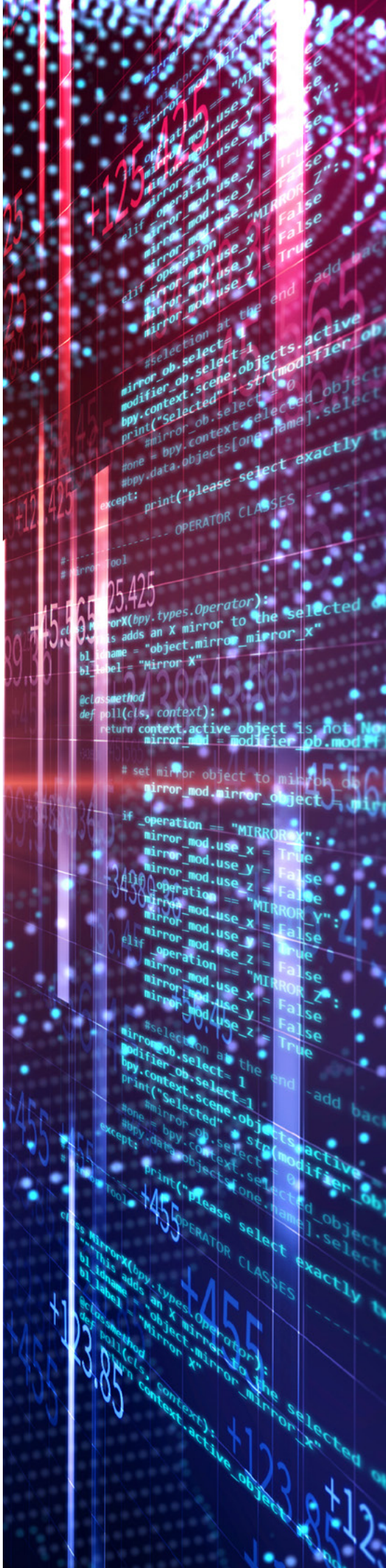
- A legal ground for processing an individual's social media data is required, such as legitimate interest. The employer should take into account (prior to inspecting the social media profile) whether the social media profile of the applicant is related to business or private purposes, and whether the collection of that data is necessary and relevant to the performance of the job which is being applied for.
- It is expected that challenges will arise in this area from unsuccessful job applicants. It could be a breach of their data protection rights if a job opportunity is withdrawn as a direct consequence of an undisclosed social media check highlighting concern.
- All of this should also apply to monitoring of existing employees' social media activity. Employers should remain proportionate in their actions and be clear within social media policies that such access may take place, if there are legitimate interests for the access.

Dark web monitoring

- Monitoring of (assumed) employees who may be active on the dark web should be fair, on lawful grounds, transparent and proportionate.
- The employer is likely to have a clear legitimate interest in seeking to prevent employees using such browsers (e.g. TOR) in an attempt for their activity to be anonymous, however the key is to achieve the monitoring using proportionate and transparent means.
- Appropriate Use policies should be clear about employees' use of the dark web, and about monitoring which may occur to ensure compliance with this policy.

Wearables

- Monitoring employees' wearables will involve the processing of health information by the employer and (even when the organisation is supplying the wearable) would be prohibited under GDPR because explicit consent is required. It is very unlikely that employees will be able to give valid explicit consent given the unequal power balance within the employment relationship.
- The view appears to be that if wearables are provided by an employer, only the employee should be able to access that information.
- The data processing should be fair, transparent and proportionate. Employees should be made aware prior to issue, and of the measures that are in place to safeguard the privacy of health information.
- It is sensible to hold the data in an anonymised format where possible (e.g. until it is requested by the employee).



Other IT monitoring considerations – discussed in passing in the main report.

- The GDPR imposes important and significant restrictions on employers in the context of employee monitoring. Importantly employers can no longer sensibly rely on an employee's consent to monitoring.
- Consider that email or instant messaging content could include personal or sensitive personal information – which may not have been disclosed to the organisation (e.g. relating to an employee's political beliefs, sexual orientation, health etc).
- Similarly, an employee may browse the internet to research, for example, health symptoms, which they may not have disclosed to their employer.
- Consider the implication of employees making claims when their organisation suffers a breach of their personal information.
- Consider that data which may be anonymous in isolation, may become personally identifiable information when aggregated with other anonymous data (e.g. when using behavioural analytics).

CPNI
Centre for the Protection of National Infrastructure

大成 DENTONS