CPNI
Centre for the Protection of National Infrastructure

OPEN AND SHARED DATA:

ADOPTING A SECURITY-MINDED APPROACH

Background

In June 2012, the UK Government published its Open Data White Paper 'Unleashing the Potential' which was aimed at:

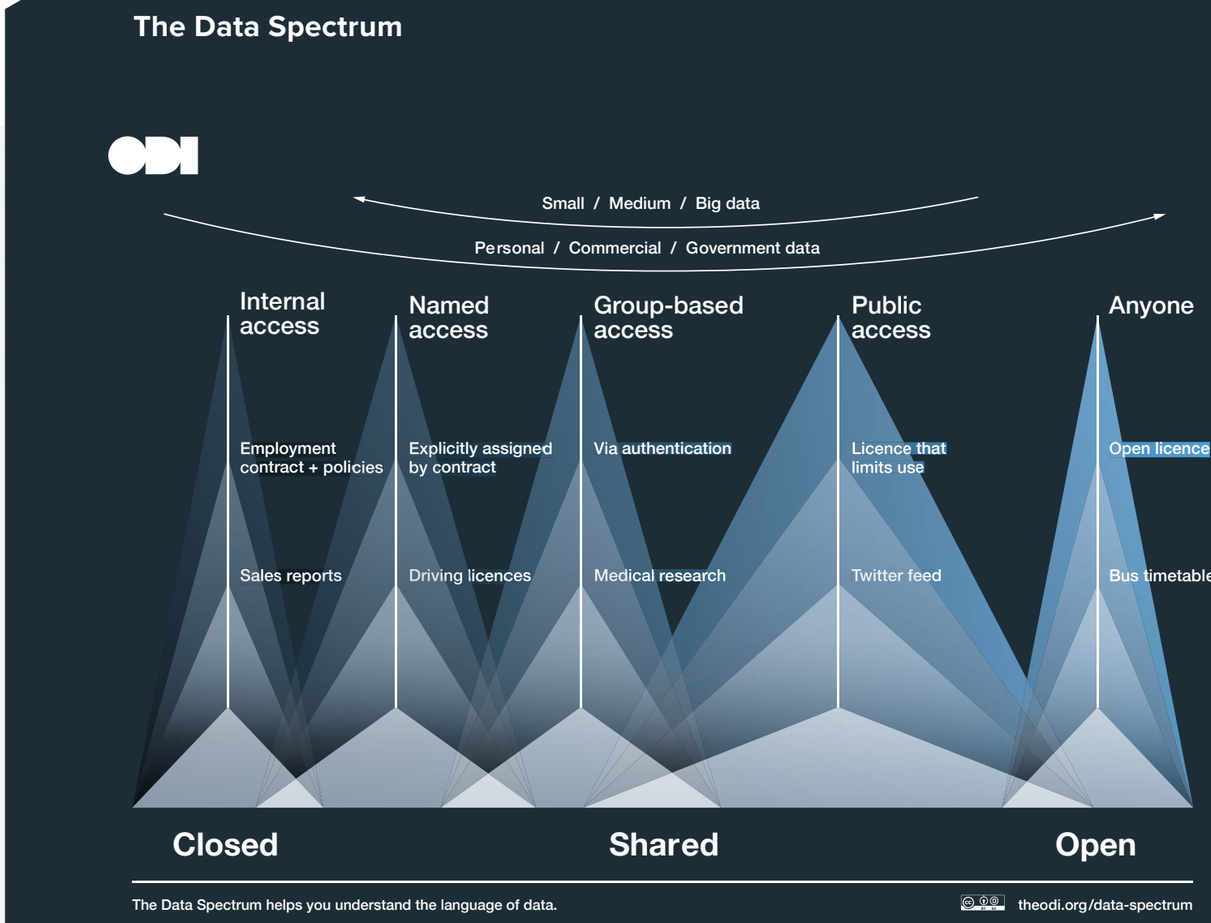
- making it easier to access public data
- making it easier for publishers to release data in standardised, open formats; and
- engraining a 'presumption to publish' unless there are clear, specific reasons (such as privacy or national security) not to do so.

The paper defined "open data" as:

- accessible (ideally via the internet) at no more than the cost of reproduction, without limitations based on user identity or intent;
- in a digital, machine readable format for interoperation with other data; and
- free of restriction on use or redistribution in its licensing conditions.

However, in recent years, "big data", "commercial data" and "personal data" increasingly feature in conversation around this topic.

The Open Data Institute (ODI) was keen to develop some clarity around all of these terms in order to facilitate the unpacking of the challenges and benefits of data. In response to this, it produced the Data Spectrum which ranges from closed to shared to open, the type of licensing requirements and examples of the types of data in each category.



This guidance provides a framework for adopting a security-minded approach to the sharing of data, including open data. Its purpose is not in any way to undermine the principles of open data or to reduce the benefits that may be gained from greater data sharing.

Available at https://theodi.org/about-the-odi/the-data-spectrum/

What do we mean by data?

Data can be defined as a series of marks, digital or analogue signals or encoded characters stored or transmitted electronically and can include writing, printed characters or graphics.

Data becomes information when one or more data items have a context, and therefore convey a message or meaning. In some cases the absence of data can also be informative, for example, the presence of redactions in a document informs the reader that there is some sensitivity regarding the redacted content.

For simplicity, in this guidance document, the term ‘data’ is used to encompass both data and information as defined above and therefore also includes maps and mapping layers.

The need for security

It is important to be aware that the sharing of certain data could:

- adversely affect the privacy, welfare, safety or security of an individual or individuals;
- compromise the safety or security of sensitive assets or the services which they exist to deliver;
- compromise intellectual property or trade secrets of an organisation;
- cause commercial or economic harm to an organisation or country; and/or
- jeopardise the security, internal and foreign affairs of a nation.

Any data which could lead to any of the outcomes outlined above should be regarded as sensitive.

Where an organisation holds sensitive data, a security-minded approach should be adopted in relation to its sharing.

A security-minded approach should be adopted when an organisation considers sharing sensitive data.

The security-minded approach

Security-mindedness is the understanding and routine application of appropriate and proportionate security measures so as to deter and disrupt unwanted, potentially security-compromising behaviours or activities.

The need for such an approach should be assessed prior to:

01 the release of a data set to a third party;

02 the sharing of a new data set;

03 the update of an existing shared data set;

04 undertaking a review of an existing data set; or

05 the augmenting or linking a new or existing data set with another data set.

Implementing a security-minded approach

An overview of the process for applying a security-minded approach is shown in Figure 1 below.

Figure 1. Overview of the process for applying a security-minded approach to data sharing

01

Identifying the need for a security-minded approach

When a decision has been taken to share a data set, the need for a security-minded approach to be applied should be assessed using the data security triage process outlined in Figure 2 to the right.

Where there is any uncertainty as to the sensitivity of data, appropriate advice should be sought. Where some data has already been shared, releasing additional data or updating existing shared data may increase the risk and/or potential harm that could occur through its hostile or malicious use.

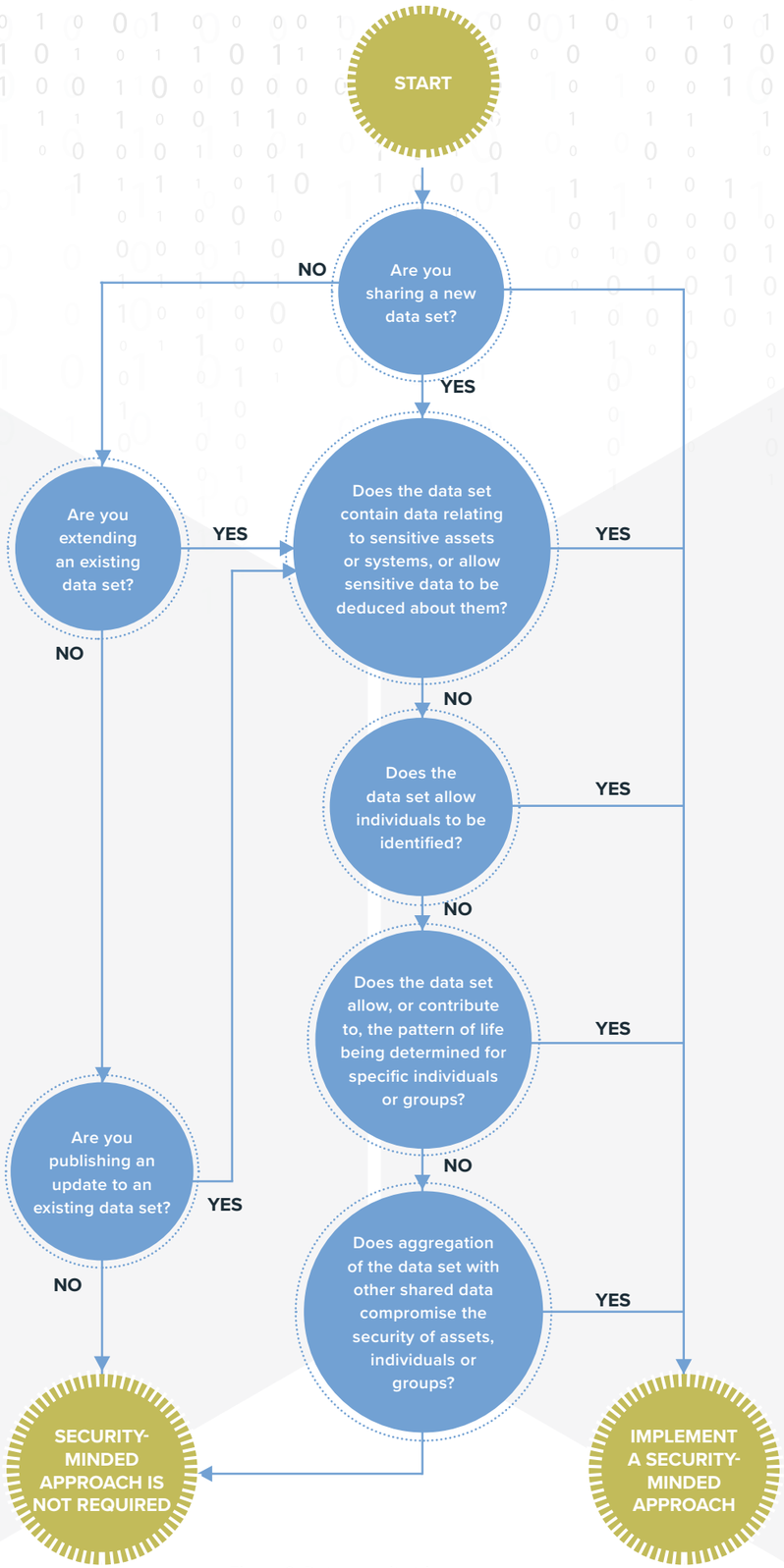


Figure 2. Data security triage process

02

Put in place data security governance structures

An individual at top management level will need to be accountable for the security-minded approach to be adopted. In addition, responsibility will need to be assigned to an individual, or individuals, for:

- identifying potential security and data aggregation issues;
- the development and management of the Security Strategy and Security Management Plan;
- advising on the need for, and undertake, the relevant monitoring and auditing;
- obtaining appropriate professional security advice where necessary.

03

Assess the security risk and develop mitigation measures

A security risk assessment should consider the potential threats and vulnerabilities arising from the sharing of data, in combination with an assessment of the nature of the harm which could be caused to:

- the asset(s), and/or service(s) that the data relates to;
- the benefits the asset(s) and/or service(s) the asset(s) exists to deliver, be they societal, environmental and/or commercial; and
- to individuals or groups.

Where the risks identified exceed an organisation's risk appetite, appropriate and proportionate security mitigation measures should be developed.

Risk mitigation measures which it may be appropriate to adopt include:

- removing a sub-set of the data from the shared data set where only that sub-set creates a security risk;
- reducing the precision of the information where the precision of location or timing data increases the security risk;
- providing the data in summary form to reduce the level of detail available where the granularity of the data increases the security risk;
- share the data set without the metadata, or remove the sensitive fields, where the metadata creates a security risk;
- reduce the level of detail and/or remove some layers of mapped data as a user zooms in to view a locality where the granularity of the data increases the security risk; and
- monitoring access by requiring user registration/login to access specific data sets.

The risk management process is not a one-off, it should be repeated periodically to ensure that the other data that has been, or is about to be, shared is identified, any impact on the original risk assessment is determined and appropriate mitigation measures are put in place.

04

Develop a Security Strategy

A Security Strategy should be developed, managed, monitored and, where required, updated. It should document:

- the security concerns and requirements determined by the security triage process;
- the data security governance arrangements;
- the security risks identified;
- the security mitigation measures to be implemented to address any unacceptable security risks;
- any tolerated security risks; and
- the mechanisms for reviewing and updating the Strategy.

The review process should identify and assess any risks which have changed for political, economic, social, technological, legal or environmental reasons and should be undertaken:

- prior to sharing of a data set;
- on a periodic basis to assess data aggregation risks;
- in the event of a security breach or incident;
- in response to the development of new tools and techniques to analyse data.

The Strategy will be a sensitive document and therefore access to it should be managed on a need-to-know basis with appropriate security measures with regards to its creation, storage, distribution and use.

05

Develop a Security Management Plan

The Security Management Plan should include:

- the policies and processes for the preparation, release, storage and dissemination of data, taking into consideration any relevant legislative or regulatory requirements;
- monitoring, auditing and review arrangements;
- a plan for handling security breaches and incidents; and
- the process for the provision of information to third parties who intend to share the data, including an outline of the contractual or licensing measures required.

As with the Security Strategy, a suitable mechanism for the periodic review of the Security Management Plan will need to be in place.

06

Information Sharing Agreements

Where data is being shared outside formal contracts it may be appropriate to put in place an Information Sharing Agreement which detail:

- the purpose(s) of the sharing;
- the potential recipients;
- the type of information to be shared;
- the quality of the information to be shared;
- the security requirements which need to be in place;
- monitoring and auditing requirements; and
- sanctions for a breach of the data/information or the Information Sharing Agreement itself.

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 favour 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 judgment as regards to the use of this document and seek independent professional advice on your particular circumstances.

CPNI

Centre for the Protection of National Infrastructure