GDPR and the Internet: Evolution not Revolution

Jon Langley
Senior Technology Officer (Technology Policy)

ico.
Information Commissioner's Office

UKNOF40
Manchester Central Convention Complex
27 April 2018

General Data
Protection Regulation
EU 2016/679

In force: **04 May 2016**

Applies: **25 May 2018**

GDPR

The key principles

1. Personal data must be processed fairly and lawfully

2. Personal data must be processed for limited purposes

3. Personal data must be adequate, relevant, and not excessive

4. Personal data must be accurate and, where necessary, kept up to date

5. Personal data must not be kept for longer than is necessary

6. Personal data must be processed in line with the data subjects' rights

7. Personal data must be processed securely

8. Personal data must not be transferred to other countries without adequate protection

DPA 1998: the Data Protection Principles

1. Personal data must be processed fairly, lawfully and transparently

2. Personal data must be processed for specific, explicit and legitimate purposes

3. Personal data must be adequate, relevant, and limited to what is necessary

4. Personal data must be accurate and, where necessary, kept up to date

5. Personal data must not be kept for longer than is necessary

6. Personal data must be processed securely

Article 5(2): Accountability Principle

The data controller shall be able to demonstrate compliance with the above

GDPR: principles relating to processing of personal data (Article 5)

DPA

'Personal data' means data which relate to a living individual who can be identified-

a) From those data, or

b) From those data and other information which is in the possession of, or likely to come into the possession of, the data controller,

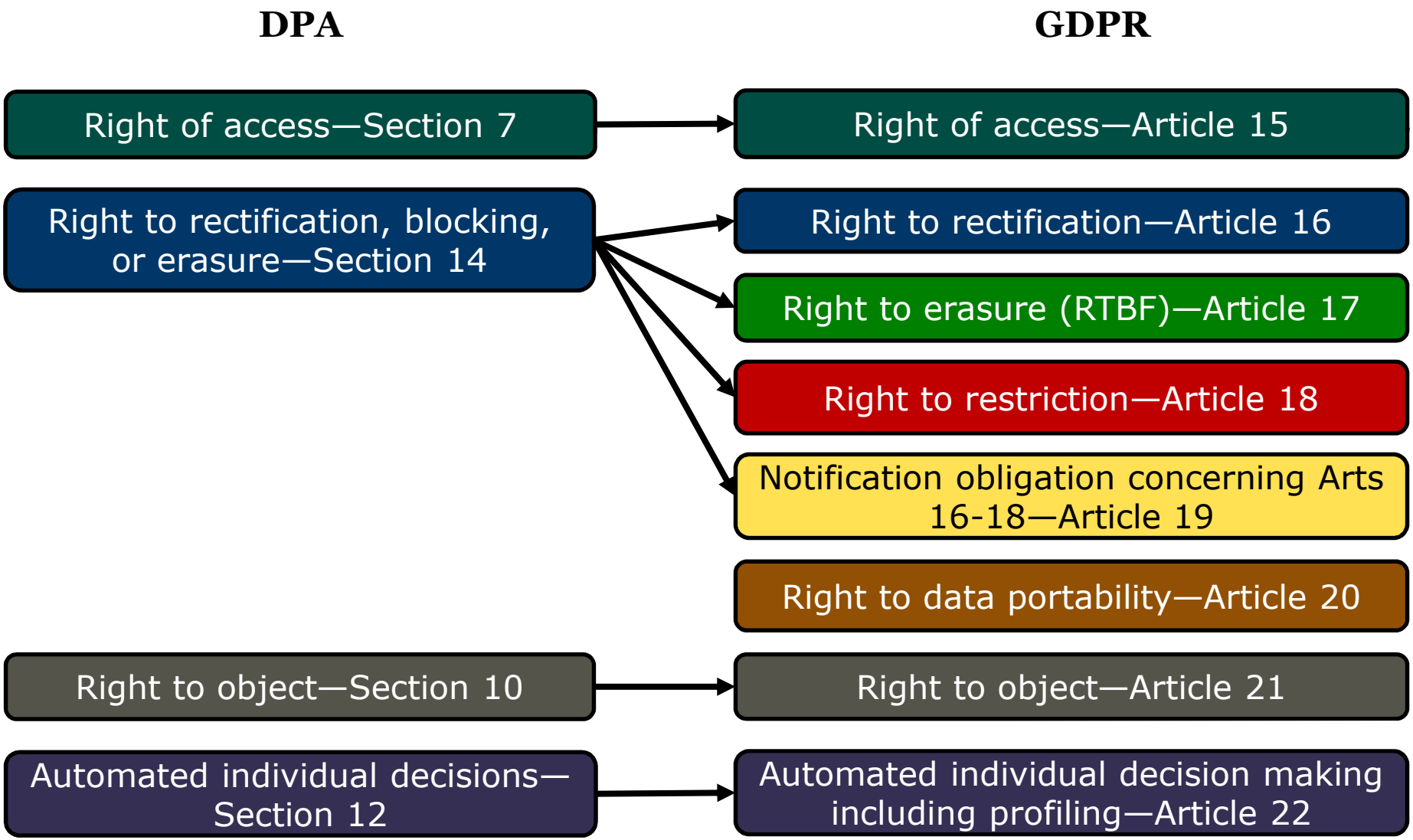
And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

GDPR

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to **an identifier such as a name**, an identification number, **location data, an online identifier** or to one or more factors specific to **the** physical, physiological, **genetic**, mental, economic, cultural or social identity **of that natural person**

Definition of personal data

Data subject rights



Data subject rights: DPA vs GDPR

Lawful bases
(Processing conditions)

DPA 1998 Schedule 2

- Consent
- Performance of a contract
- Compliance with a legal obligation
- Vital interests
- Performance of a task carried out in the public interest
- Legitimate interests

GDPR Article 6

- Consent
- Performance of a contract
- Compliance with a legal obligation
- Vital interests
- Performance of a task carried out in the public interest
- Legitimate interests

DPA>GDPR: processing conditions

So what is the position on consent?

Some specifics

Understanding the right to erasure: The Right to be Forgotten (RTBF)

The right to erasure

- One or more Article 17(1) grounds must apply:
  - Data no longer necessary
  - Data subject withdraws consent – and no other basis applies
  - Data subject objects – and no overriding legitimate grounds for continuing
  - Processed unlawfully
  - Erased for compliance with legal obligation
  - Collected in relation to information society services aimed at children

When does RTBF apply?

- Processing necessary for:
  - Exercising freedom of expression and information
  - Compliance with a legal obligation or performance of a task in the public interest
  - Reasons of public interest in the area of public health
  - Archiving purposes/scientific/historical research/statistical purposes
  - Establishing/exercising/defending legal claims

Article 17(3)

- What about…
  - Backups? Blockchain?

- Check:
  - Is the RTBF request valid? - Article 17(1)
  - Is the processing necessary? - Article 17(3)

- RTBF **may still apply** and you **may have to take steps to comply.**

Specific technologies?

Data Processors

Articles 28 and 32

Article 32:

'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller ***and the processor*** *shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…'*

New liabilities

GDPR and other laws

General Data Protection Regulation
EU 2016/679

Network and Information Systems (NIS) Directive
EU 2016/1148

Applies to *the processing of personal data*

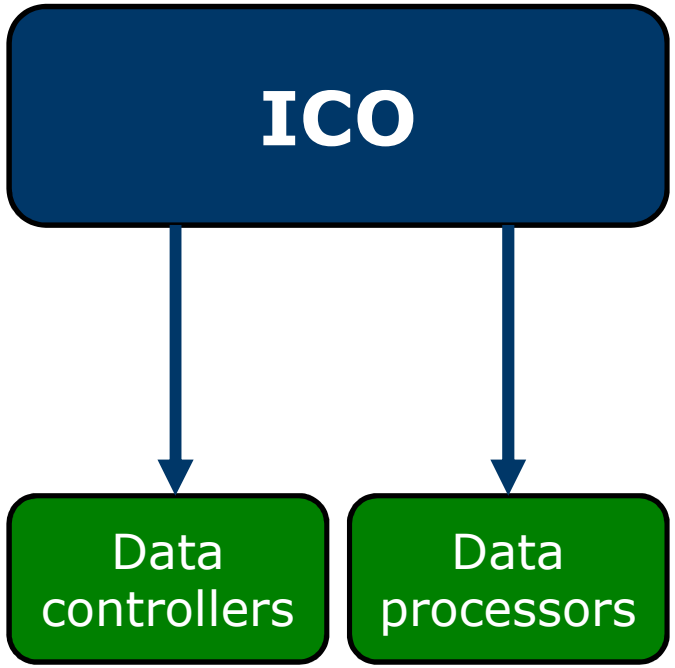
—Data controllers
—Data processors

Applies to *the security of networks and information systems*

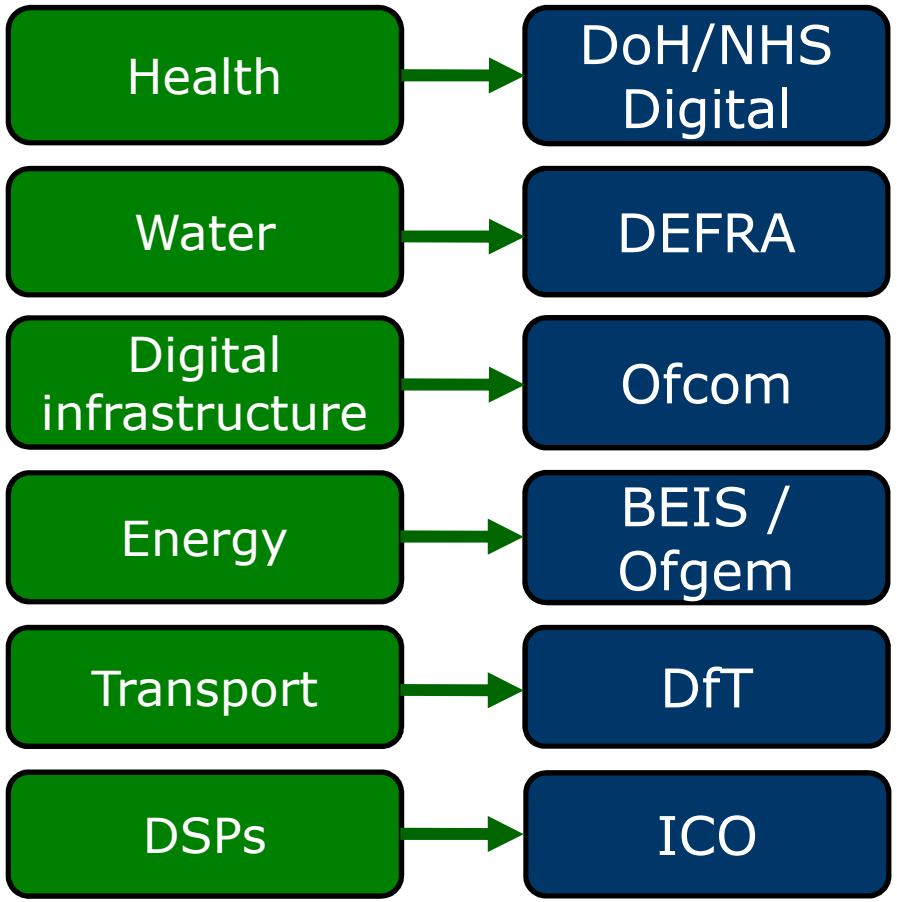
—'Operators of essential services'
—'Digital service providers' (DSPs)

GDPR and the NIS Directive

GDPR: one 'Supervisory Authority'



NIS: multiple 'Competent Authorities'



GDPR and NIS: the regulators

OES

- Section 11(1) – OES to notify 'without undue delay' their CA of:

'…incidents having a significant impact on the continuity of the essential services they provide'

DSPs

- Section 12(3) – DSPs to notify 'without undue delay' their CA of:

'…any incident having a substantial impact on the provision of any of the digital services… that it provides'

NIS: incident notification

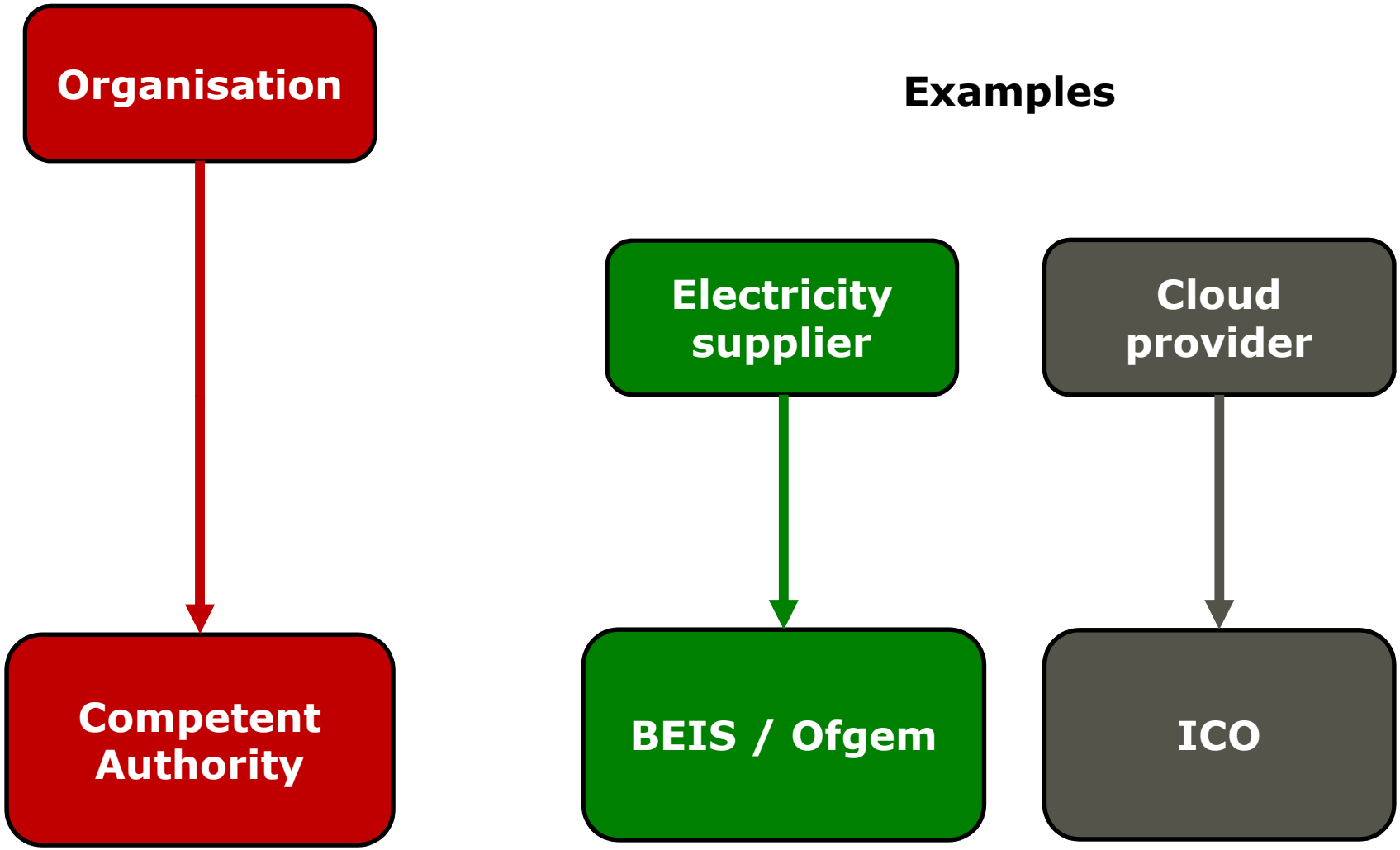
GDPR Article 4(12)—Personal data breach

'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'

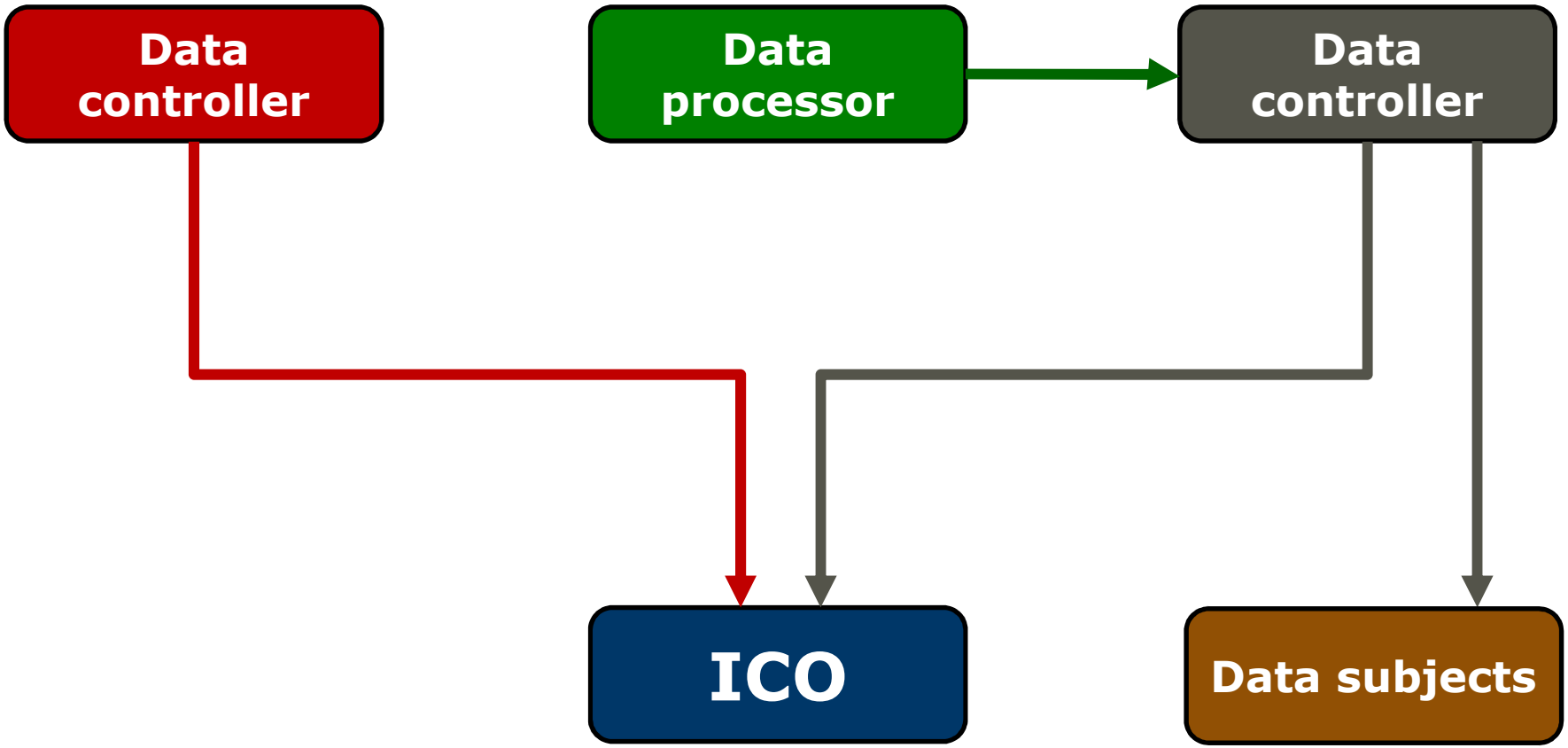
NIS Regulations Section 1(1)—Incident

'Any event having an actual adverse effect on the security of network and information systems.'

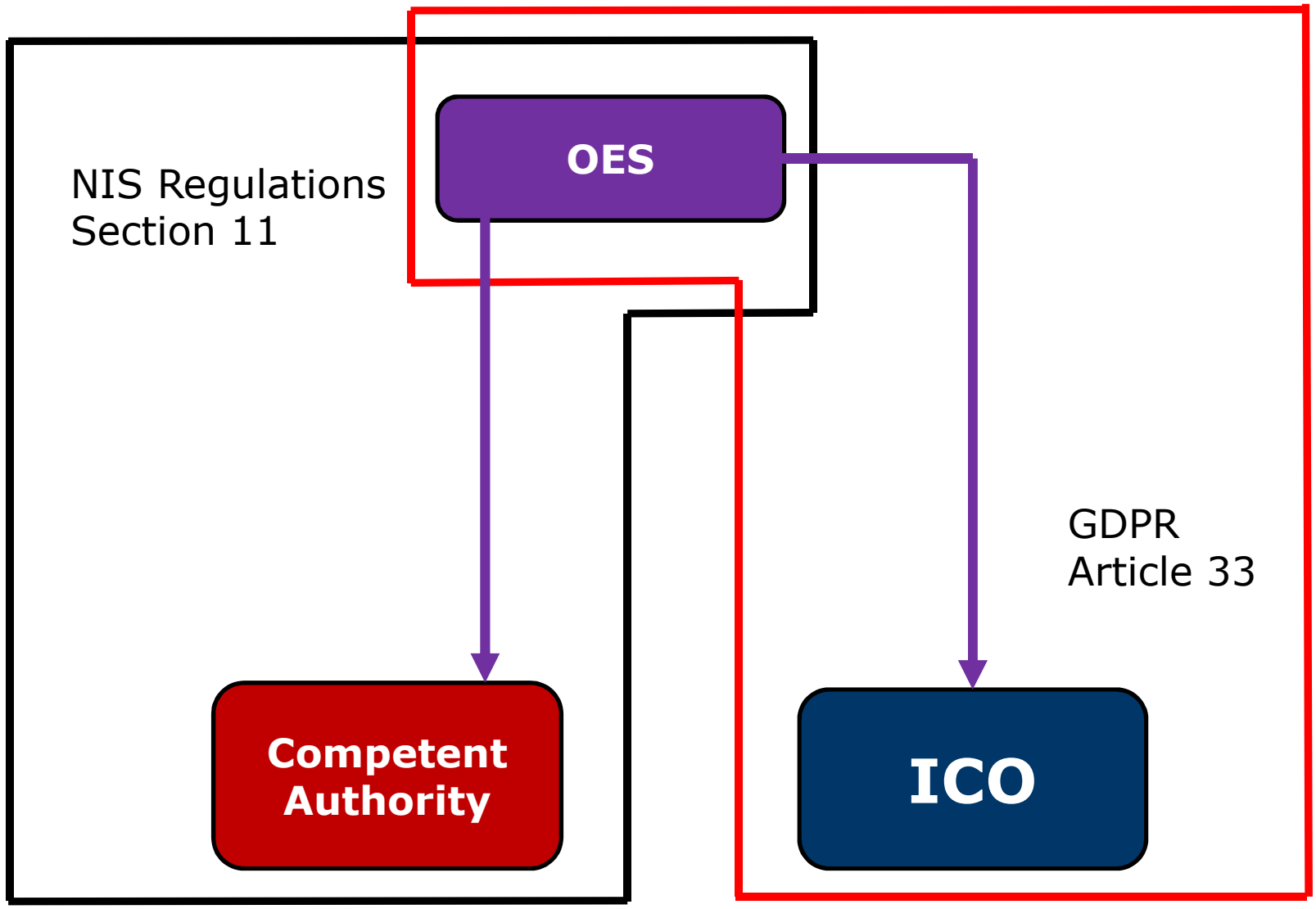
Incidents vs. personal data breaches



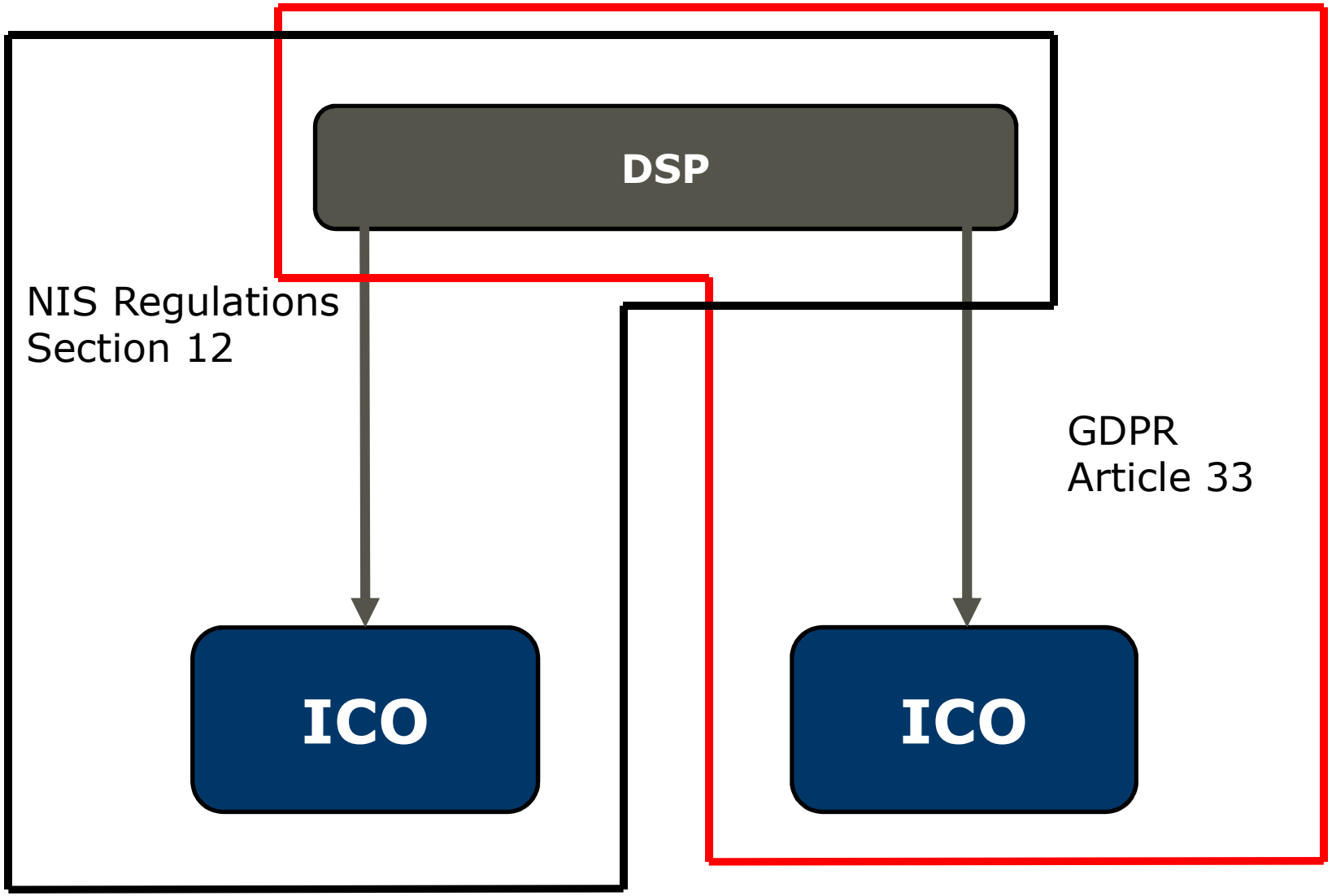
Incident notification under NIS



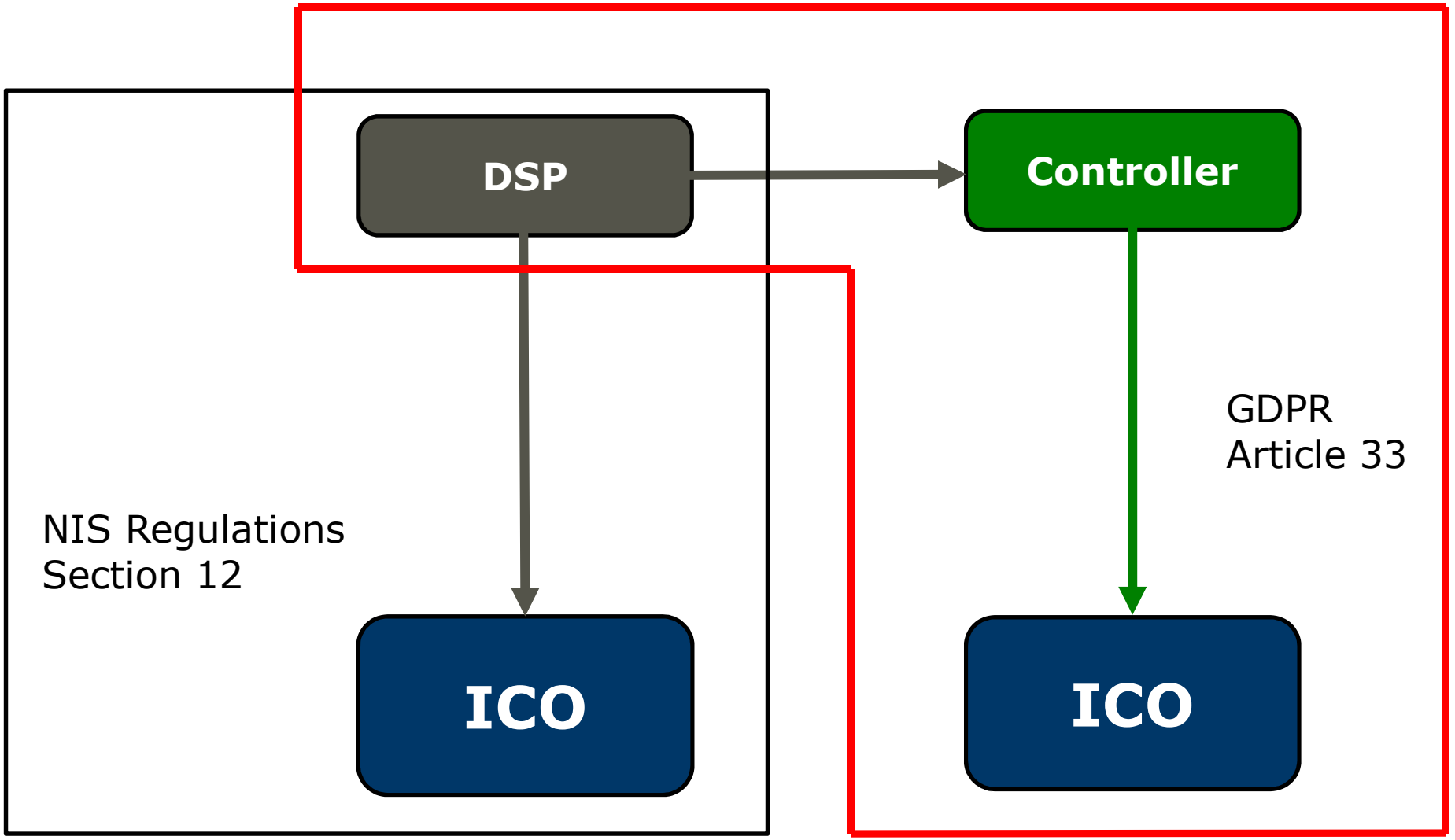
Notification under GDPR



When a NIS incident is also a breach of personal data processed by an OES (OES = data controller)



When a NIS incident is also a breach of personal data processed by a DSP (DSP=data controller)



When a NIS incident is also a breach of personal data processed by a DSP on behalf of another (data processor)

Personal data breach notification

- Nature of breach
- Numbers and categories of data subjects
- Numbers and categories of personal data records
- Name and contact details of DPO
- Likely consequences
- Measures taken to address the breach / mitigate the adverse effect

NIS incident report

(i) the operator's name and the essential services it provides;
(ii) the time the NIS incident occurred;
(iii) the duration of the NIS incident;
(iv) information concerning the nature and impact of the NIS incident;
(v) information concerning any, or any likely, cross-border impact of the NIS incident;
and
(vi) any other information that may be helpful to the competent authority;
and

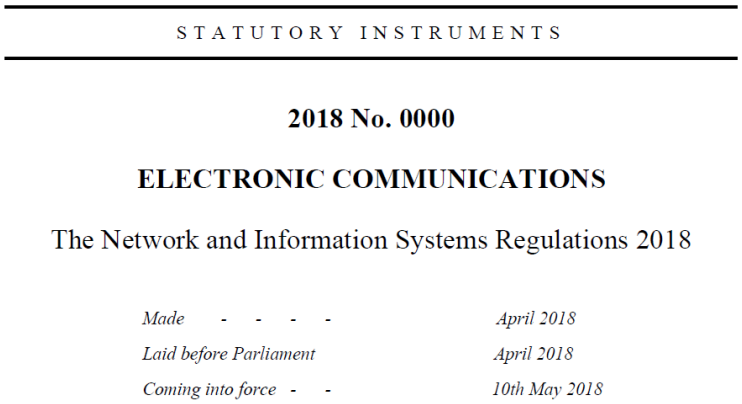
Comparison

- Difference can be summarised as follows:

> "All personal data breaches are security incidents, but not all security incidents are personal data breaches"
>
> Article 29 Guidelines on breach notification

- NIS concerns *disruption* to services: not all incidents will involve personal data.
  - But those that do would still require notification under the GDPR.

GDPR vs NIS



STATUTORY INSTRUMENTS

2018 No. 0000

ELECTRONIC COMMUNICATIONS

The Network and Information Systems Regulations 2018

Made - - - -	*April 2018*
Laid before Parliament	*April 2018*
Coming into force - -	*10th May 2018*

- Incident reporting:
  - To harmonise with GDPR
  - Within 72 hours
  - For both OES and DSPs
- Penalty regime
  - No longer to mirror GDPR
  - Penalties of up to £17m, no penalty based on turnover
- Co-operative approach
  - Example: a 'NIS incident involving loss of personal data'

Other details

Guidance

Data protection self assessment toolkit

with new GDPR checklist

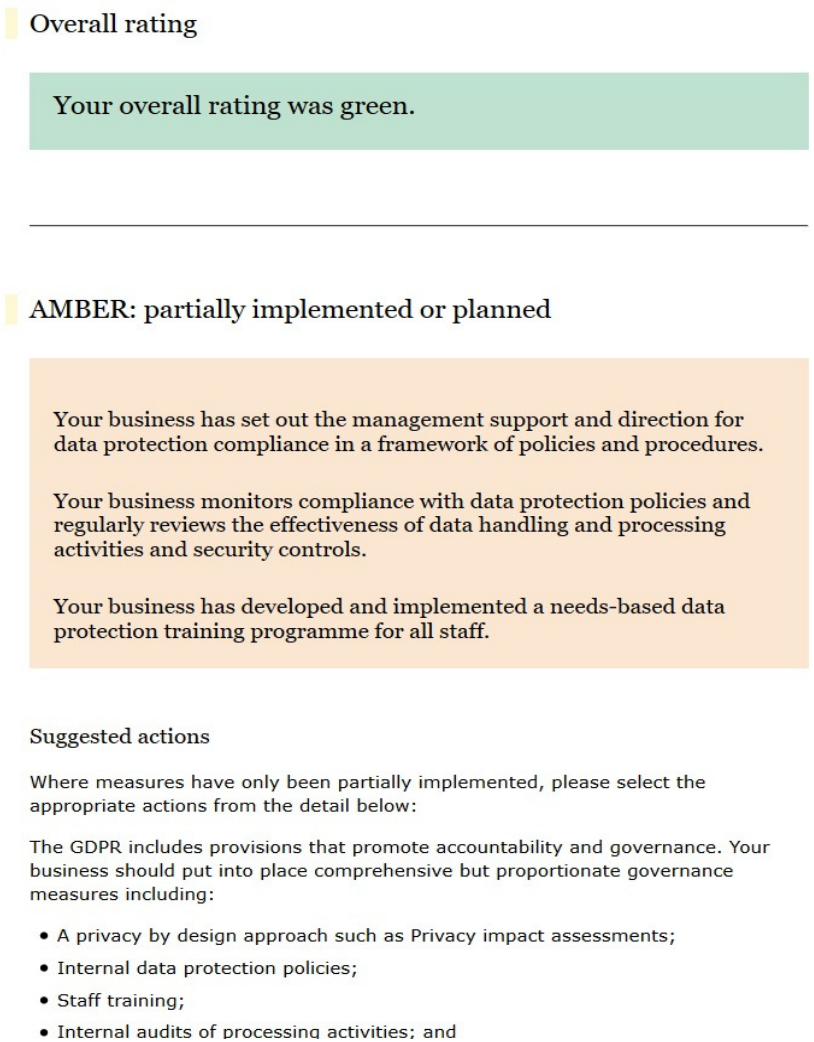
ico.
Information Commissioner's Office

Toolkits

Five step process:

1. Accountability and governance
2. Key areas to consider
3. Individuals' rights
4. Breach notification
5. International

Provides overall rating and suggestions for improvement (where applicable)



Overall rating

Your overall rating was green.

AMBER: partially implemented or planned

Your business has set out the management support and direction for data protection compliance in a framework of policies and procedures.

Your business monitors compliance with data protection policies and regularly reviews the effectiveness of data handling and processing activities and security controls.

Your business has developed and implemented a needs-based data protection training programme for all staff.

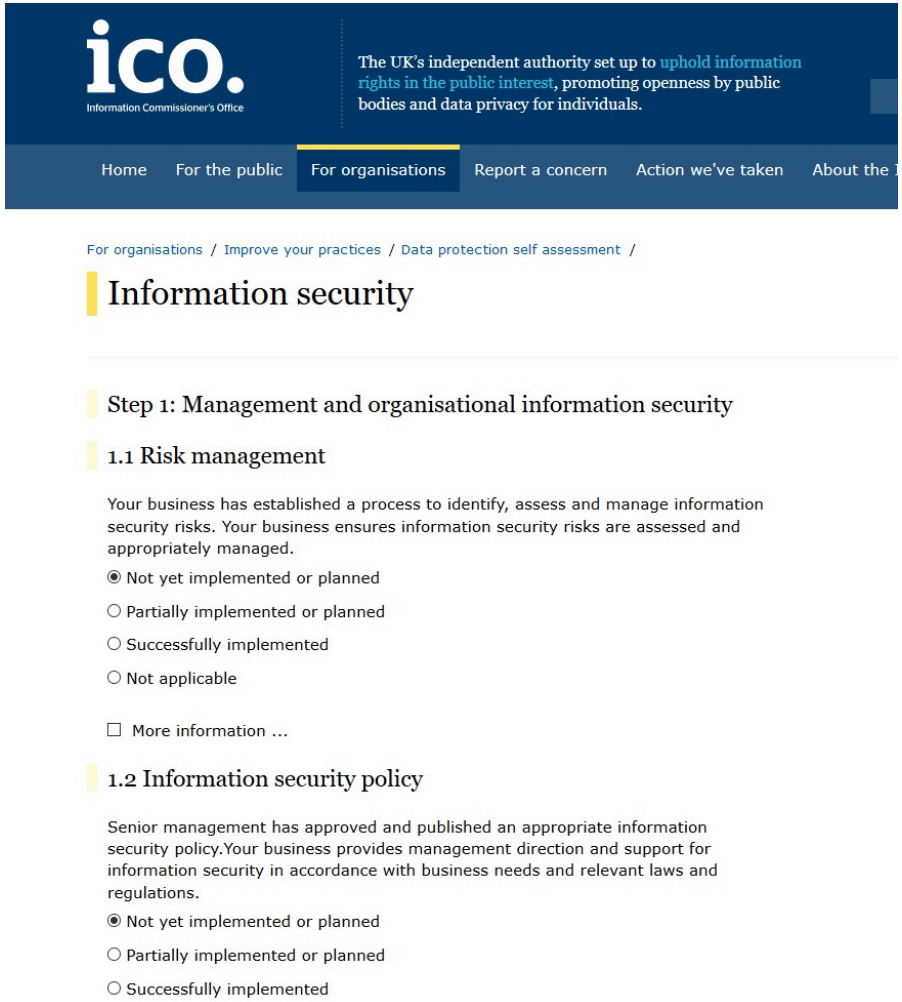
Suggested actions

Where measures have only been partially implemented, please select the appropriate actions from the detail below:

The GDPR includes provisions that promote accountability and governance. Your business should put into place comprehensive but proportionate governance measures including:

- A privacy by design approach such as Privacy impact assessments;
- Internal data protection policies;
- Staff training;
- Internal audits of processing activities; and

Getting ready for the GDPR



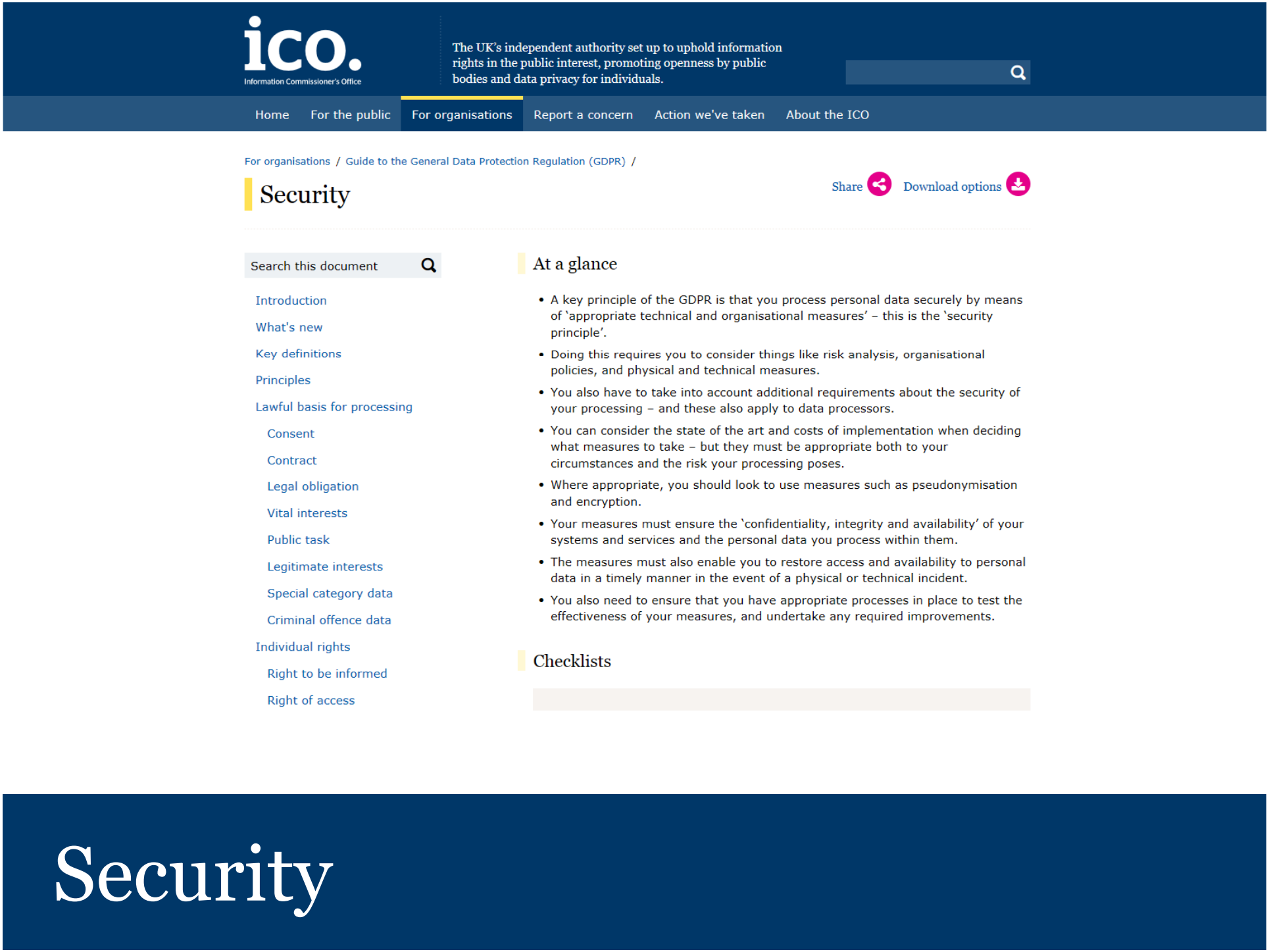
Four step process:

1. Management and organisational information security
2. Staff and information security awareness
3. Physical security
4. Computer and network security

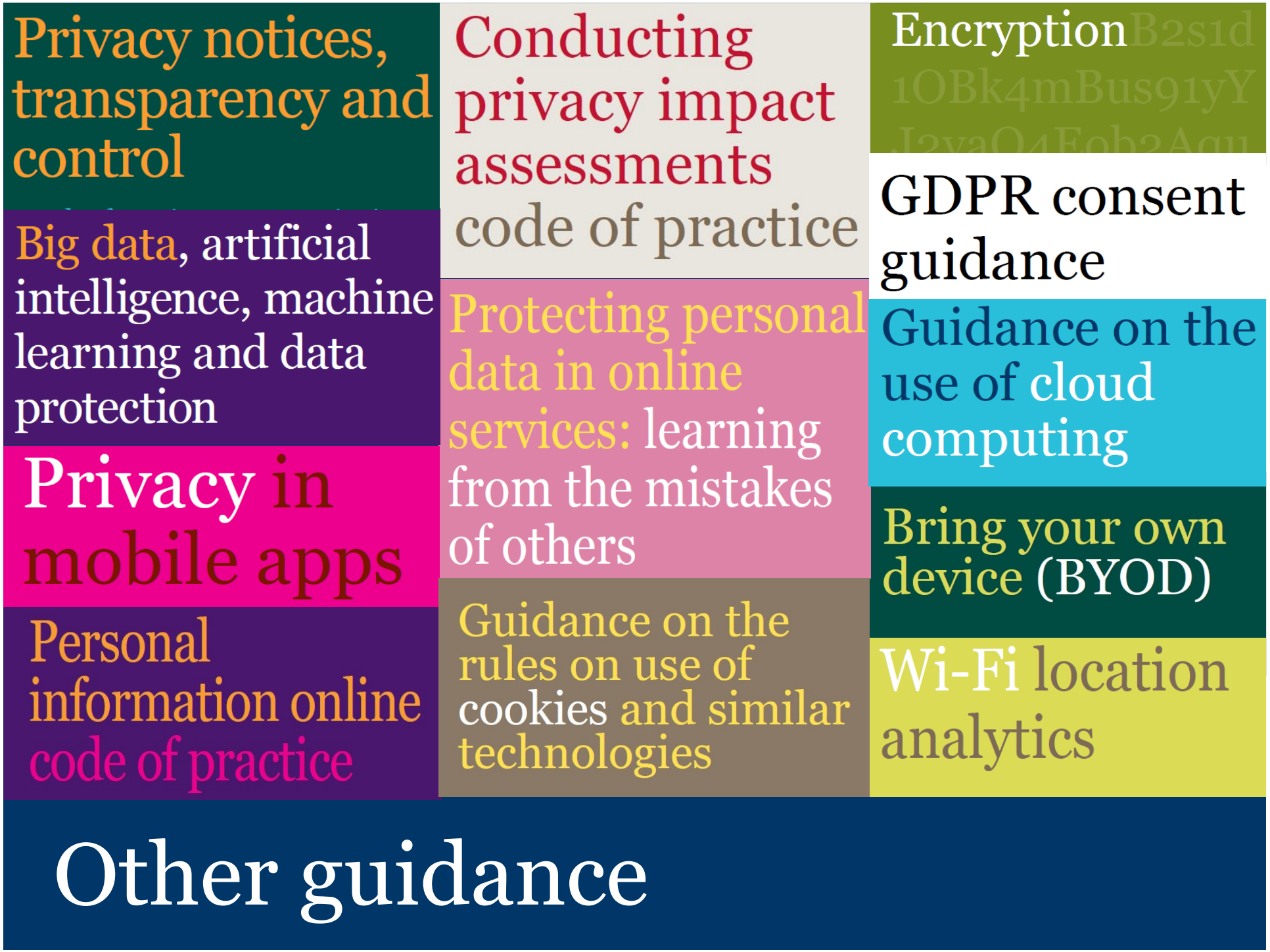
Provides overall rating and suggestions for improvement (where applicable)

Information security assessment

Guide to GDPR


ico.
Information Commissioner's Office
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Home
For the public
For organisations
Report a concern
Action we've taken
About the ICO
For organisations / Guide to the General Data Protection Regulation (GDPR) /
Security
Share
Download options
Search this document
Introduction
What's new
Key definitions
Principles
Lawful basis for processing
Consent
Contract
Legal obligation
Vital interests
Public task
Legitimate interests
Special category data
Criminal offence data
Individual rights
Right to be informed
Right of access
At a glance
A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.
Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.
You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
Where appropriate, you should look to use measures such as pseudonymisation and encryption.
Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.
Checklists

Security


Privacy notices, transparency and control
Conducting privacy impact assessments code of practice
Encryption
GDPR consent guidance
Big data, artificial intelligence, machine learning and data protection
Protecting personal data in online services: learning from the mistakes of others
Guidance on the use of cloud computing
Privacy in mobile apps
Bring your own device (BYOD)
Personal information online code of practice
Guidance on the rules on use of cookies and similar technologies
Wi-Fi location analytics
Other guidance

ARTICLE 29 DATA PROTECTION WORKING PARTY

Published:

- WP242rev01 Guidelines on data portability
- WP243rev01 Guidelines on data protection officers
- WP244rev01 Guidelines on lead authority
- WP248rev01 Guidelines on data protection impact assessments
- WP250 Guidelines on breach notification
- WP251 Guidelines on profiling
- WP259 Guidelines on consent
- WP260 Guidelines on transparency

Article 29 guidance

Summary

- GDPR is an evolution, not a revolution
  - Many of the underlying concepts and principles are well-established
- There are opportunities for organisations that get it right
  - But change may be required nonetheless
- More guidance is on the way

Keep in touch

jonathan.langley@ico.org.uk

Subscribe to our e-newsletter at **ico.org.uk**, or find us on…

/iconews

/icocomms

/company/information
-commissioner’s-office

@iconews