GDPR and the Internet: Evolution not Revolution

Jon Langley
Senior Technology Officer (Technology Policy)
General Data Protection Regulation
EU 2016/679

In force: 04 May 2016

Applies: 25 May 2018
The key principles
DPA 1998: the Data Protection 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
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

**DPA**
- Right of access—Section 7
- Right to rectification, blocking, or erasure—Section 14
- Right to object—Section 10
- Automated individual decisions—Section 12

**GDPR**
- Right of access—Article 15
- Right to rectification—Article 16
- Right to erasure (RTBF)—Article 17
- Right to restriction—Article 18
- Notification obligation concerning Arts 16-18—Article 19
- Right to data portability—Article 20
- Right to object—Article 21
- Automated individual decision making including profiling—Article 22
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

RTBF
Understanding the right to erasure

GDPR and the NIS Directive
The interplay

Data processors
Your new responsibilities
Understanding the right to erasure:
The Right to be Forgotten (RTBF)
The right to erasure (the right to be forgotten)

In brief...

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
• 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
• 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
• 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.
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...’
GDPR and other laws
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies to the processing of personal data</td>
<td>Applies to the security of networks and information systems</td>
</tr>
<tr>
<td>— Data controllers</td>
<td>— ‘Operators of essential services’</td>
</tr>
<tr>
<td>— Data processors</td>
<td>— ‘Digital service providers’ (DSPs)</td>
</tr>
</tbody>
</table>

GDPR and the NIS Directive
GDPR and NIS: the regulators

**GDPR: one ‘Supervisory Authority’**

- **ICO**
  - Data controllers
  - Data processors

**NIS: multiple ‘Competent Authorities’**

- Health
  - DoH/NHS Digital
- Water
  - DEFRA
- Digital infrastructure
  - Ofcom
- Energy
  - BEIS / Ofgem
- Transport
  - DfT
- DSPs
  - ICO
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’
Incidents vs. personal data breaches

**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.’
Incident notification under NIS

Organisation

Competent Authority

Examples

Electricity supplier

BEIS / Ofgem

Cloud provider

ICO

Incident notification under NIS
Notification under GDPR

Data controller

Data processor

ICO

Data controller

Data subjects

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)

- NIS Regulations Section 12
- GDPR Article 33
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
• 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
• 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’
Guidance
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 in 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
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)
Guide to the General Data Protection Regulation (GDPR)

Introduction

The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.

This is a living document and we are working to expand it in key areas. It includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU’s Article 29 Working Party. The Working Party includes representatives of the data protection authorities from each EU member state, and the ICO is the UK’s representative.

Alongside the Guide to the GDPR, we have produced a number of tools to help organisations to prepare for the GDPR:

- GDPR: 12 steps to take now
- Getting ready for the GDPR checklist
Security

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
Privacy notices, transparency and control

Big data, artificial intelligence, machine learning and data protection

Privacy in mobile apps

Personal information online code of practice

Conducting privacy impact assessments code of practice

Protecting personal data in online services: learning from the mistakes of others

Guidance on the use of cloud computing

Bring your own device (BYOD)

Guidance on the rules on use of cookies and similar technologies

Wi-Fi location analytics

Other guidance

Encryption

GDPR consent 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...

facebook
youtube
linkedin
twitter