EU Regulation 2016/679, GDPR

GDPR, the DPA98 on Steroids
Full title

What it’s about ...
- on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Known to one and all as ...
- The GDPR, and comprises;
  - Recitals, and
  - Articles.

Comes into force, and be applicable from ...
1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. It shall apply from 25 May 2018.

Yes, it’s already in force!

Ref: Reg EU 2016/679 Title; Article 99
REGULATION (EU) 2016/679 of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

It shall apply from 25 May 2018

Article 99

Reference:
- OJEU - Regulation (EU) 2016/679
- OJEU - Directive (EU) 2016/680
- OJEU - Directive (EU) 2016/681

Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive

Article 63

DIRECTIVE (EU) 2016/680 of 27 April 2016
on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

For commencement see Article 21 and Article 22

DIRECTIVE (EU) 2016/681 of 27 April 2016
on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime
• Applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

• Applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to
  • The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  • The monitoring of their behaviour as far as their behaviour takes place within the Union. [think about web usage, email usage, IP and MAC addresses that are monitored, BYOD or COPE usage, and in fact any other monitoring of employees – LBPR 200]

• Applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law

Ref: Reg EU 2016/679 Title; Article 3
Personal Data

- Means any information relating to an identified or identifiable natural person (‘data subject’), where
- 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.

Special categories of personal data

- Processing of personal data revealing
  - racial or ethnic origin,
  - political opinions,
  - religious or philosophical beliefs, or
  - trade union membership, and
  - the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
  - data concerning health or
  - data concerning a natural person's sex life or sexual orientation, shall be prohibited, unless....(see Article 9.2)

Ref: Reg EU 2016/679 Title; Article 4 and 9.1
Article 5 - Principles relating to processing of personal data.

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (1(a))
2. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (1(f))
3. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (1(b))
4. Kept in a form which permits identification of data subjects for no longer than is necessary (1(e))
5. Adequate, relevant and limited to what is necessary (1(d))
6. Accurate and, where necessary, kept up to date (1(c))

Source: GDPR, 2016/679
RECAP ➔ SECURITY CONCEPTS

- Security by Default
- Security by Design
- Consequence of a loss of C-I-A of information and or data
- Data minimisation
- Security over technology
- Accountability
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
- controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia...

The 'level of risk' - being the magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood (ISO Guide 73:2009)

Managing information risk

- Process:
  - Risk Assessment
    - Risk Identification
    - Risk Analysis
    - Risk Evaluation
    - Risk Treatment Options
    - Modify (level of risk)
    - Retain
    - Avoid
    - Share

- Treat the risk (apply controls - being a measure that is modifying risk): assess controls; review; monitor; communicate.

- Article 40 - Codes of Conduct
- Article 42 - Certification

Chapter VIII Remedies, Liability, Penalties

Sources:
- Regulation(EU) 2016/679 GDPR
- ISO/IEC 27005:2011
RECAP → LAWFULNESS (OF PROCESSING), AND CONSENT

One of more of the following must be in place for lawfulness of processing

- Must be able to demonstrate that consent has been obtained
- Performance of a contract to which the data subject (DS) is a party
- Compliance to legal obligations
- Protection of the vital interests of the DS, or another person
- In the public interest or, exercise of official authority vested in a data controller (DC)
- Necessary for the legitimate interest of the DC or 3rd party except where such interests are overridden by the rights of the DS (child, for example)

- Demonstrate consent has been given
- Consent can be withdrawn
- Written consent must be clearly distinguishable from other conditions using clear and easily accessible language
- Within a contract, consent only applies to data necessary to fulfil that contract
- Consent of children can only be given by someone having parental rights
**DATA PROTECTION BILL**


  **Vision ...**

  *to make the UK the safest place to live and do business online.*

New criminal offences will be created to deter organisations from either intentionally or recklessly creating situations where someone could be identified from anonymised data.

Data protection rules will also be made clearer for those who handle data but they will be made more accountable for the data they process with the priority on personal privacy rights.

The Bill will bring the European Union’s General Data Protection Regulation (GDPR) into UK law, helping Britain prepare for a successful Brexit

Make it easier and free for individuals to require an organisation to disclose the personal data it holds on them

Make it easier for customers to move data between service providers (should be fun for the IT teams)

Address the derogations stated in the GDPR

Ref: Department for Digital, Culture, Media and Sport A New Data Protection Bill: Our Planned Reforms
NO QUICK FIXES

• Take into account the simple facts;
  • DPA98 → COMMENCEMENT ORDER, JUNE 2000.
    • Every, relevant organisation (public or private) had 2 years to implement requirements. Did they?
      • An audit of an organisation’s Information Security Management System (ISMS) for Certification to ISO/IEC 27001:2013 requires many elements to be in place, one of which is knowledge of sensitive and or critical information and data – PII (in the context of GDPR).
        • Do organisations have an information asset register?
        • Have data owners actually taken responsibility for the risk to PII?
        • Do data owners work closely with the custodian (call it IT) regarding the location of data?
        • Has the level of risk to PII been truly understood and managed, and by whom?
        • What is the stakeholder’s tolerance to risk?
        • What about the DPIA? (sure, not an actual requirement under DPA98)
        • What about resilience (RTO and RPO)?
      • Many organisations will fail at the basics. This was all covered under P7 of the DPA98. Article 32 is harder hitting.
In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. (Recital 84)

Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing. (Recital 84)

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment. (Article 35)
• ‘Adequacy’ and 3\textsuperscript{rd} Country
  • UK remains within the EU, at the moment.
  • BREXIT will mean the UK becomes a 3\textsuperscript{rd} Country with regard to the GDPR.
  • UK must prove ‘adequacy’
    • Legal process, within the EU, that cannot happen until UK leaves the Union.
    • Therefore ...
    • Gov. (and the ICO) must do all in their power to ensure that the UK’s new Data Protection legislation is able to successfully negotiate the legal process to gain ‘adequacy’ status.
    • The Data Protection Bill and any future amendments should be addressing this challenge.

• Note
  • Data Protection Law Enforcement Directive (DPLED), in contrast to the GDPR, is not “directly applicable” EU law. This means that the UK must implement its provisions prior to 6 May 2018. These will be written into the new Bill.
LINKS - ADDENDUM

- GDPR
  - ICO link
  - EU Site
- Law Enforcement Directive
- ICO Sub-site, GDPR
- Handy iOS version
  - DLA Piper (provides detail on the Articles with relevant links to Recitals)
- Handy Guide, from DLA Piper
  - https://www.dlapiper.com/~/media/Files/Insights/Publications/2016/12/General%20Data%20Protection%20Regulation%20Brochure.PDF
Certificate in Information Security Management Principles (CISMP)
- 5 Day Public scheduled course
- Carlisle or Penrith (TBC) – 2nd to 6th of October 2018
- £850.00 per delegate, includes the BCS Exam, all course material, tea/coffee during the day, and lunch.
For more information: contact@kansecurity.com

Acuity
STREAM Cyber Risk Platform
Fast, flexible, scalable and easy to use GRC software for Cyber Risk Management
https://www.acuityrm.com/

LRQA
Lloyd's Register
Countdown to Transition
If you still need to transition to the new ISO 9001 and ISO 14001 standards, attend Live 2017
0800 328 6543
Book now
http://www.lrqa.co.uk/events/live17/

Contact: contact@kansecurity.com