GDPR: The new legal framework governing data protection

Angela Oakley, GDPR / Data Protection Consultant

Overview

- Enhanced definitions of Personal Data and Consent
- The responsibilities of Data Controllers and Data Processors
- Data Breach notification
- The role, position and responsibilities of Data Protection Officers
- Increased individual rights

Headlines

- The General Data Protection Regulations (GDPR) come into force in the UK on 25th May 2018
- The new legal framework in the EU which includes significant enhancements to the UK Data Protection Act (DPA) 1998 which will be repealed once GDPR comes into effect.
- The UK Data Protection Bill will include a 'GDPR scheme' ensuring the principles of the Regulations are enshrined in UK Data Protection Law
- Regulations introduce a principle of 'accountability' requiring that organisations must demonstrate compliance
- The financial penalties have been significantly increased from the current maximum fine of £500,000 to 20 million Euros or 4% of the organisations' annual turnover, whichever is highest – this equates to around £18m at the current exchange rate. Fines for non-compliance with Regulations as well as Data Breaches

6 GDPR Principles

Data Protection Act 1998 (Schedule 1)	General Data Protection Regulations (Article 5)
1. Processed fairly and lawfully	a) Lawfulness, fairness and transparency
2. Processed for specified reasons	b) Purpose Limitation
3. Adequate, relevant and not excessive	c) Data Minimisation
4. Accurate and up to date	d) Accuracy
5. Not kept for longer than necessary, for the purpose(s) it is used	e) Storage Limitation
6. Uphold Data Subject Rights	Articles 12 to 23 increased individual rights under GDPR
7. Appropriate technical and organisational security measures	f) Integrity and Confidentiality
8. Not transferred outside of EEA without adequate protection	Article 3 – Territorial scope

Enhanced Definitions
Personal Data

Data Protection Act 1998 (section 1(1))	General Data Protection Regulations (Article 4(1))
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 is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual	**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

‘Special Categories’ of Personal Data

Data Protection Act 1998 (Part 1, Section 2) ‘Sensitive Personal Data’	General Data Protection Regulations (Article 9(1))
(a) The racial or ethnic origin of the data subject	Racial or ethnic origin
(b) His political opinions	Political opinions
(c) His religious beliefs or other beliefs of a similar nature	Religious or philosophical beliefs
(d) Whether he is a member of a trade union	Trade union membership
(e) His physical or mental health or condition	Genetic data Biometric Data for the purpose of uniquely identifying a natural person Data concerning health
(f) His sexual life	Data concerning a natural person’s sex life or sexual orientation
(g) The commission or alleged commission by him of any offence, or	
(h) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings	

Consent

Definition has been strengthened with data controllers now having to be able to evidence that consent is 'valid'.

"any freely given, specific, informed and **unambiguous** indication of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action,** signifies agreement to the processing of personal data relating to him or her"

For consent to be considered 'valid' it must be:

- Freely given; this means giving people genuine ongoing choice and control over how you use their data
- Information provided to Data Subjects before they are able to provide consent must specifically cover the Data Controller's name, the purposes of the processing and the types of processing activity
- Must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly
- Should be obvious and require a positive action to opt in
- Explicit consent must be expressly confirmed in words, rather than by any other positive action
- There is no set time limit for consent. How long it lasts will depend on the context and should be reviewed and refreshed as appropriate

Data Controller / Data Processors

- "*Controller* – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data…“
- "*Processor* - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

Data Processor obligations

- Controller / Processor contract
- Demonstrating compliance – ‘accountability’
- Security – ‘technical and organisational security measures’
- Breach notification – to Data Controller
- Data Protection Officer (in certain processing situations)
- Codes of Conduct

Data Breaches

- Article 31 of the GDPR provides that *"in the case of a personal data breach[1], data controllers shall without undue delay"* and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority unless the personal data breach is *"unlikely to result in a risk for the rights and freedoms of individuals"*.

  If a notification is not made within 72 hours of the data breach, the data controller must give a 'reasoned justification' explaining the reason for the delay. Additional obligations are also imposed on data processors to notify the data controller after becoming aware of a personal data breach[2]. The data controller is also required to record any personal data breaches and any actions that the data controller has taken in respect of that.

Data Breaches

Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller is required to communicate the nature of the personal data breach together with the information set out above, in clear and plain language, to the data subject concerned, without undue delay.

There are however some circumstances when the notification to the data subject is not required, including

- The controller has implemented appropriate technical and organisational protection measures in respect of the personal data affected by the breach (such as encryption).
- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of individuals is no longer likely to arise.
- It would involve disproportionate effort.

Data Protection Officer

Obligatory for public authorities or where processing on a large scale or special categories data

Must be independent (although they can be a member of staff or contractor)

Must report to the highest management level of the organisation – within Public Authorities this will be the Board of the organisation

Must have expert knowledge of data protection law and practices, and the ability to perform the tasks specified in the GDPR

- Article 37 – Designation of the data protection officer
- Article 38 – Position of the data protection officer
- Article 39 – Tasks of the data protection officer

Data Protection Officer
Article 39 - Tasks

Article 39(1) Tasks	Evidence – 'Accountability' principle
(a) Inform and advise organisation and staff of responsibilities	Policies, Procedures and other measures to ensure compliance Keeping records of processing activities
(b) Monitor compliance	Training and staff awareness Reports of compliance to DPO
(c) Provide advice where requested regarding the Data Protection Impact Assessment, and monitor performance	DPO to advise on DPIAs where 'high risk' processing and mitigations proposed
(d) Cooperation with the ICO	Reporting of data breaches, includes non-compliance with Regulations
(e) Contact point with ICO	Where 'high risk' processing and mitigations proposed following advice from DPO

Data Protection Impact Assessments

Obligatory where:

- New technologies are to be introduced
- Processing is likely to result in a high risk to the rights and freedoms of data subjects
- Evaluation of personal aspects based on automated processing
- processing on a large scale of special categories of data (includes health and genetic data)
- systematic monitoring of a public area (CCTV, for example)

Article 35 provides a list of what the DPIA should contain including a description of the envisaged processing, an assessment of the necessity and proportionality of the processing, an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks.

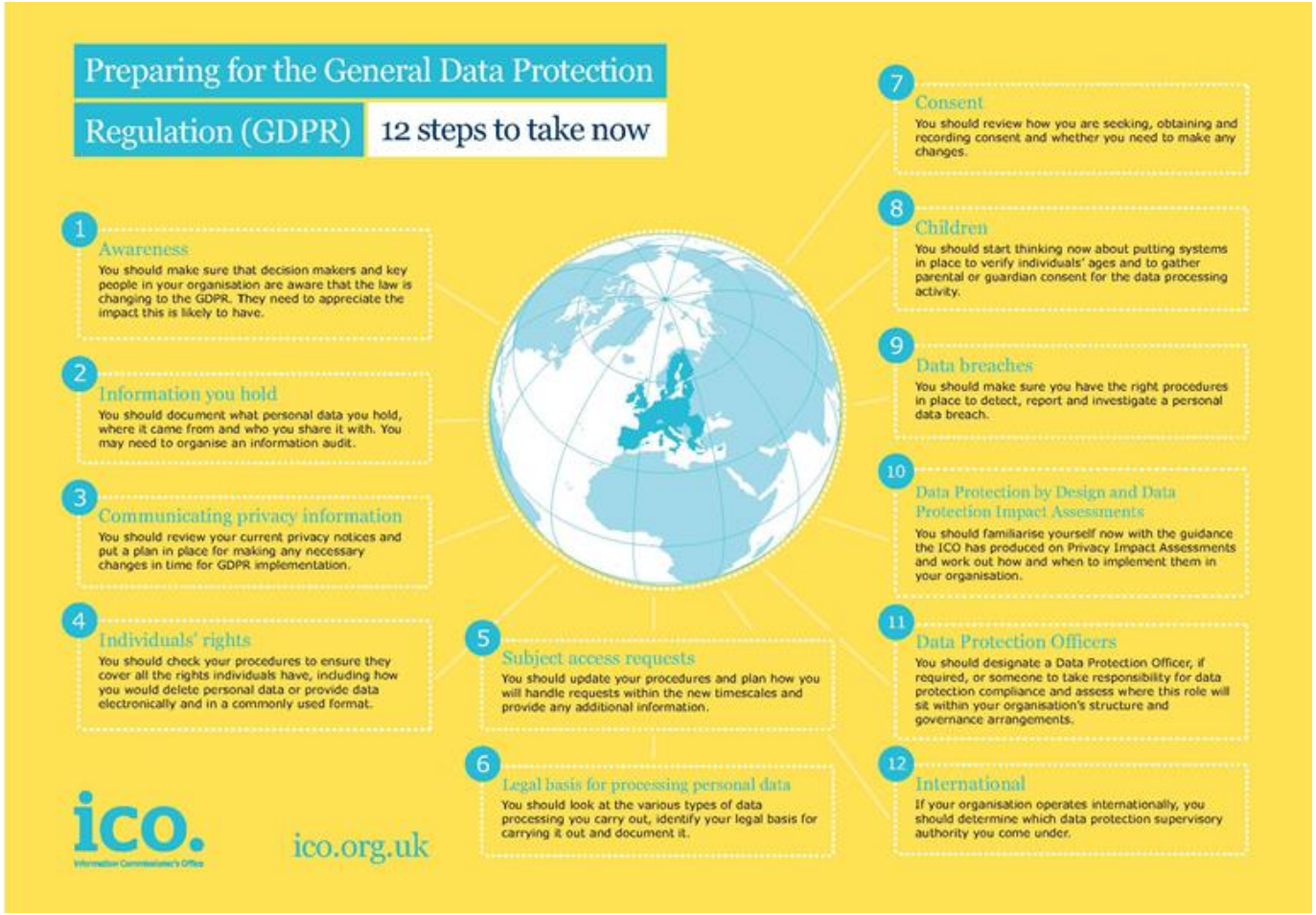
After the impact assessment has taken place, in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remain high), the data controller must consult the ICO as per Article 36.

Individual Rights

Articles 12 to 23 Increased individual rights under GDPR

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Preparing for the GDPR: ICO 12 Steps to take now



Thank you, any questions?

Angela Oakley, GDPR / Data Protection Consultant