The General Data Protection Regulation – how to deal with personal data fairly and lawfully

Elinor Corbett-Jones, Associate Solicitor
3 May 2018

HUGH | JAMES

Understanding law, understanding you

Overview

- 25 May 2018 despite Brexit
- Instantly in force as a Regulation – but a UK Data Protection Bill has been published
- Largely similar to current Data Protection Act 1998, but sufficiently different to be grabbing headlines
- Much bigger fines
  - €10m or 2% of global turnover
  - €20m or 4% of global turnover
- Other associated legislation: Regulation on Privacy and Electronic Communications (currently in draft)

Agenda

- Personal data – what are we talking about
- Data protection principles
- Key steps in getting ready for the GDPR
  - Data mapping
  - Legal bases for processing
  - Individual rights
  - Privacy notices
- Demonstrating compliance
- Breaches and the duty to notify

Personal data

- Any information relating to an “identifiable living individual”
- Means a living individual who can be identified, directly or indirectly, in particular by reference to:
  - an identifier such as a name, ID number, location data an on-line identifier; or
  - one or more or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual
- Previous definition in the DPA confirmed that it includes:
  - Expressions of opinion
  - Indication of intentions

High risk personal data

Identified as a special category of data:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Offences or alleged offences
- Physical or mental health
- Genetic data
- Biometric identification data
- Sexual life
- Sexual orientation

High risk data: electronic communication data, location data, financial data (that might be used for payment fraud)

Data protection principles

1. Processing must be lawful, fair and transparent
2. Collected for specified, explicit & legitimate purposes
3. Adequate, relevant and not excessive for the purposes
4. Accurate and kept updated
5. Kept for no longer than necessary in an identifiable form – retention policy
6. Kept securely – appropriate organisational and technological methods that protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

- Processed in line with individuals' rights
- Not transferred outside EEA

Getting ready for the GDPR

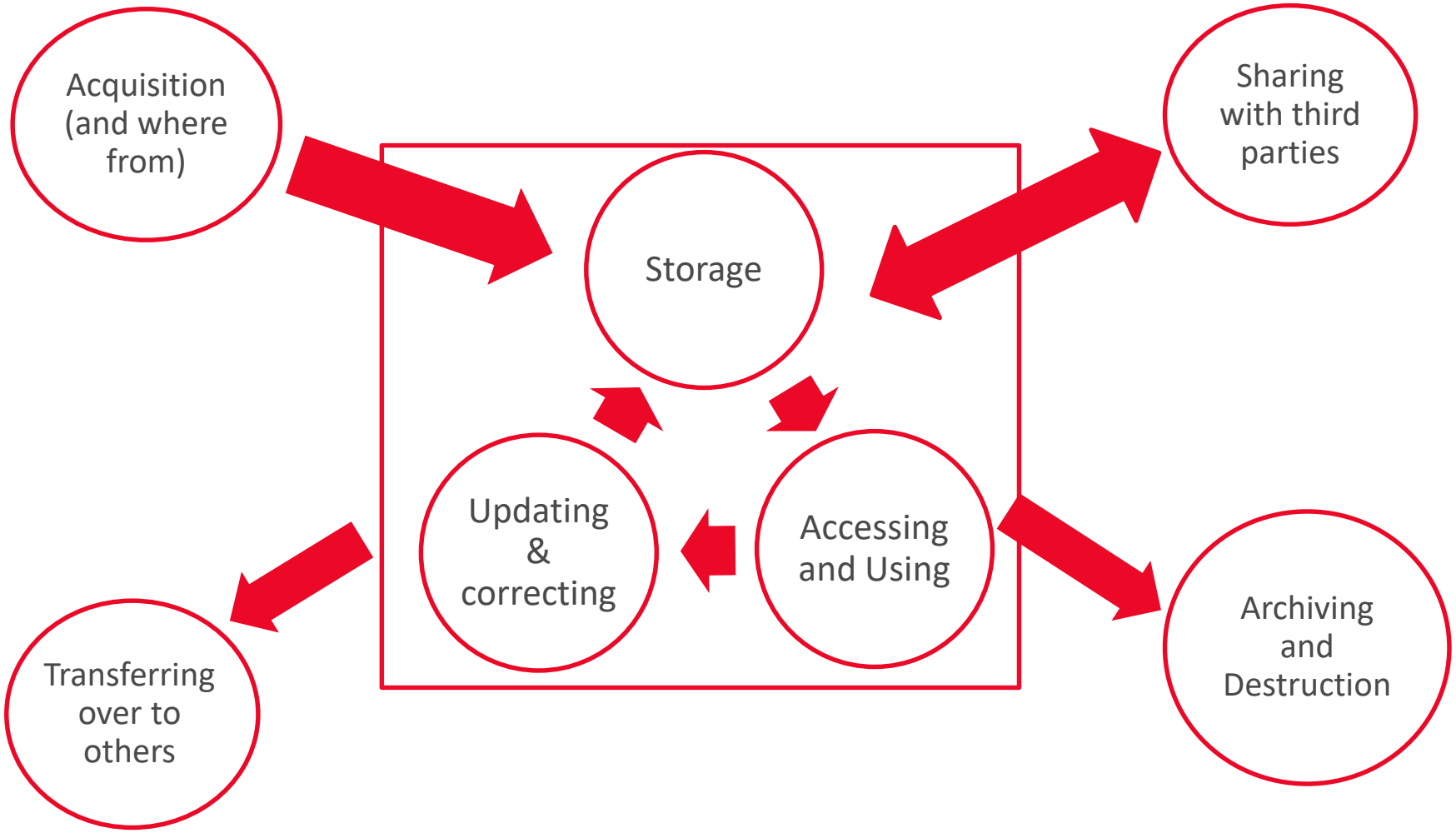
What personal data do we process and why?

Which GDPR legal bases are we relying on?

Therefore: which individual rights apply?

Draft your privacy notices

The data journey – stages of processing



Data controllers and data processors

- Data controller – the natural or legal, public authority, agency or other body which alone, or jointly with others, determines the purposes and means of processing personal data

- Data processor – a legal entity who processes personal data on behalf of the controller (other than a person employed by the controller)
  - Rules about the selection of data processors and contracts with them

- N.B. can often be difficult to unravel – it is possible to have joint controllers of the same information

Legal basis (ordinary personal data)

1. Consent
2. Necessary for the performance of a contract – with the data subject
3. Necessary for a legal obligation
4. Necessary to protect the vital interests of the data subject or another person
5. Necessary for the performance of a task in the public interest or in the exercise of official authority
6. Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

Legal basis (special categories personal data)

- Explicit consent
- Preventing or detecting crime / preventing fraud
- Regulatory activities
- Public functions
- Employment law, social security law or law relating to social protection
- Employment benefits (life insurance / pensions)
- Monitoring equal opportunities (race, disability, sexual orientation and religion)

Consent under the GDPR

- High standard whereby individuals have genuine choice and control
- Clear and concise - specific and granular, not vague or blanket consent
- Requires a positive affirmation – consent by default is not acceptable
- Implied consent is still possible, but limited
- Should be kept separate from other terms and conditions
- It should not be a precondition of a service
- Easy to withdraw
- Demonstrable via records – who, when, how, and what you told people

Consent when direct marketing - RPEC

- Must have prior consent for **all** marketing via electronic communications
- Marketing has a very broad definition
- Previous distinction between individual and corporate subscribers to be removed
- The previous customer provision has been retained:
  - Where you have acquired the contact details in the context of the sale of a product or a service, you can market a similar product or services without prior consent
  - The previous reference to negotiating has been removed
- Must (a) identify itself as a marketing communication
  (b) identify the data controller and (c) provide an easy unsubscribe option
- N.B. cookies

Individual rights

- The right to be informed – Privacy Notices
- The right of access
- The right to rectification
- The right to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

- N.B. lots of complex exemptions including for example “crime and taxation”, legal proceedings, regulatory functions, exam marks

How do individuals enforce the rights?

- Approach the data controller:
  - Positive obligation to assist the data subject
  - One month to react (can potentially extend to two months)
  - Must not charge (although there are some exceptions)
  - Must tell the data subject of further rights
- Complaint to the ICO
- Court action and a claim for compensation – includes damages for distress (material and non material damage)

Privacy Notices – when and how?

When

- At the time the data is acquired directly from the data subject
- If acquired from a different source:
  - within a reasonable period – no later than a month; or
  - if using for communication with the data subject, at the time of the first communication; or
  - If disclosing to a third party, when the data are first disclosed

How

- Written information
- Concise, transparent, intelligible, easily accessible, written in clear and plain language (children) and free of charge
- Layered approach – print / electronic

Privacy Notices – what?

- Identity of the data controller – contact details
- Purposes and the *legal basis* for the processing
- Categories of personal data
- Potential recipients – who we share it with - by name
- Details of transfers outside the EEA
- Retention period (criteria to be used)
- Existence of the *individual rights* – and which ones apply
- *The right to withdraw consent*
- The right to lodge a complaint
- The source of the data - if not directly acquired
- Consequences of failing to provide data
- Automated decision making and profiling

Accountability – demonstrating compliance

- Relationship with the ICO
- Record keeping
- Data Protection Officer?
- Data protection by design and default
- Use Data Processors
- Data protection impact assessments (DPIAs)

Record keeping

- Baseline for all clear, comprehensive data protection policies

Organisations with 250+ staff – record of processing

- Purposes of your data processing
- Description of the categories of data and data subjects
- Categories of recipients
- Transfers outside EAA
- Retention policy
- A general description of your security measures

Record keeping

Smaller organisations – record of processing

- Only where processing is likely to result in a risk to data subjects
- Not occasional
- Includes special categories

Data Protection Officers

- Mandatory in three circumstances
  1. Public authority
  2. Large scale systematic monitoring of individuals
  3. Large scale processing of special categories of data

- Likely to be 27,000 appointed across Europe on day one

- Proper responsibility / important role
  - Point of contact
  - Inform and advise
  - Monitor compliance
  - Report to highest management level

H | J

Data protection by design and default / DPIA

- Idea that data protection should be embedded into processes from the start

- Data Protection Impact Assessment (DPIA) - current good practice as a risk management tool to assess the impact of processing on a data subject

- GDPR makes a DPIA an express legal requirement in certain circumstances:
  - When using new technologies
  - When processing is likely to result in high risk to rights and freedoms of individuals

H | J

Breaches and compulsory notifications

- Breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data – more than just losing data
- Where likely to result in a *risk* to the rights and freedoms of individuals
- Possible risk of : discrimination, damage to reputation, loss of confidentiality, significant financial loss or significant economic or social loss.
- Every breach has to be assessed to see if it hits that threshold
- 72 hour notification timescale
- May also need to notify the data subjects themselves – *"high risk"*
  - Potential fine of €10m Euro if fail to notify
  - Potential fine of €20m Euro for the breach itself

Criminal offences – Data Protection Act 2018

- **Section 117** – obstructing an ICO inspection or to failing to assist the inspection
- **Section 139** - failing to comply with an information notice or knowingly or recklessly providing a false statement
- **Section 161** – knowingly or recklessly to obtaining, disclosing, retaining, selling or offering to sell personal data without the consent of the controller
- **Section 162** – knowingly or recklessly re-identifying de-identified personal data without the consent of the controller
- **Section 163** – altering, defacing, blocking, erasing, destroying or concealing information so as to prevent disclosure under a data access request

QUESTIONS

Thank you for listening

CONTACT

Lowri Walters
Senior Associate
lowri.walters@hughjames.com
029 2039 1038

Elinor Corbett-Jones
Cyfreithiwr Cyswllt
Elinor.jones@hughjames.com
029 2010 3968

hughjames.com