GDPR: one year on

14 November 2019

Overview

1. Welcome and introduction
2. Recap: key changes under the GDPR
3. One year on: what have we learned about the GDPR?
4. Q&A

Recap: key changes under the GDPR

Kelly Fraser

Senior Associate

The legislation

- The GDPR stands for the General Data Protection Regulation (EU) 2016/679, which governs the use of personal data across the EU
- The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (the DPA)
- The DPA supplements the GDPR, implements the EU Law Enforcement Directive and extends data protection laws to areas not covered by the GDPR
- Both the GDPR and DPA applied from 25 May 2018
- The Information Commissioner's Office (the ICO) is the supervisory authority for data protection in the UK
- BREXIT – the UK Government intends to incorporate the GDPR into UK data protection law when the UK leaves the EU

The legislation

- The GDPR and the DPA apply to the processing of personal data that is:
  - Processed wholly or partly by automated means
  - The processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system
- Personal data includes information re natural persons who can be:
  - Identified, or who are identifiable, directly from the information in question
  - Indirectly identified from that information in combination with other information
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and may be processed in more limited circumstances

Refresher of key changes under the GDPR

- Data protection principles
- Lawful processing
- Data subjects' rights
- Data Protection Officers
- Data protection by design and by default

Data protection principles

- The GDPR sets out seven key principles:
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (security)
  - Accountability
- Measures to demonstrate firms' compliance include: policies, data protection impact assessments; contracts; and records

Lawful processing

- Lawful basis from list in the GDPR must be identified before processing of personal data by firms
- Processing of special categories of personal data by firms needs a lawful basis and special condition to be identified before processing
- Consider:
  - What is the purpose of your processing, what are you trying to achieve?
  - Can it reasonably be achieved in a different way?
  - Do you have a choice over whether or not to process?
  - Are you a public authority?

Data subjects' rights

- The rights of individuals under the GDPR are as follows:
  - Right to be informed
  - Right of access
  - Right to rectification
  - Right to erasure
  - Right to restriction
  - Right to data portability
  - Right to objection
  - Rights re automated decision making and profiling
- Legal responsibility on firms to identify requests and handle them accordingly

Date subjects' rights

- One month to respond calculated as follows:
  - If a request is received by a firm on 1 November 2019, the time limit starts on the same day (whether or not this is a working day)
  - The deadline for responding will be the corresponding day of the following month, in this case, 1 December 2019
  - As 1 December 2019 is a Sunday, the deadline is the next working day, 2 December 2019
- Restrictions on data subjects' rights under the DPA:
  - Exemption from data protection principles (except lawful basis) and data subjects' rights re disclosure under law or in legal proceedings
  - Exemption from data protection principles, right to be informed and right of access re legal professional privilege
  - Exemption from data protection principles, right to be informed and right of access re negotiations with data subject

Data Protection Officer (DPO)

- Firms must appoint a DPO if core activities involve processing special categories of personal data on large scale or regular and systematic monitoring of data subjects on large scale
- The duties of the DPO are to:
  - inform and advise firms on obligations to comply with the GDPR
  - monitor compliance with data protection legislation and policies, including managing activities, raising awareness, training and audits
  - advise on and monitor data protection impact assessments
  - be the first point of contact for and cooperate with the ICO
- In the performance of their tasks, the DPO shall take into account the risk associated with processing operations and the nature, scope, context and purposes of the processing

Data protection by design and default

- By design
  - Having appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights
  - Integration of data protection into processing activities and business practices throughout lifecycle
- By default
  - Only processing personal data that is necessary to achieve specific purpose
  - Specification of personal data before processing starts
  - ‘Privacy first’ approach

Data protection by design and default

- Record of processing activities
  - ICO templates for controllers and processors
  - Organisations with < 250 employees only need to record information for:
    - Processing that is likely to result in a risk to the rights and freedoms of data subjects
    - Processing that is not occasional
    - Processing of special categories of personal data
  - Must record:
    - Firm details
    - Purposes of processing and categories of data subjects and personal data
    - Recipients and transfers
    - Retention periods and security measures

Data protection by design and default

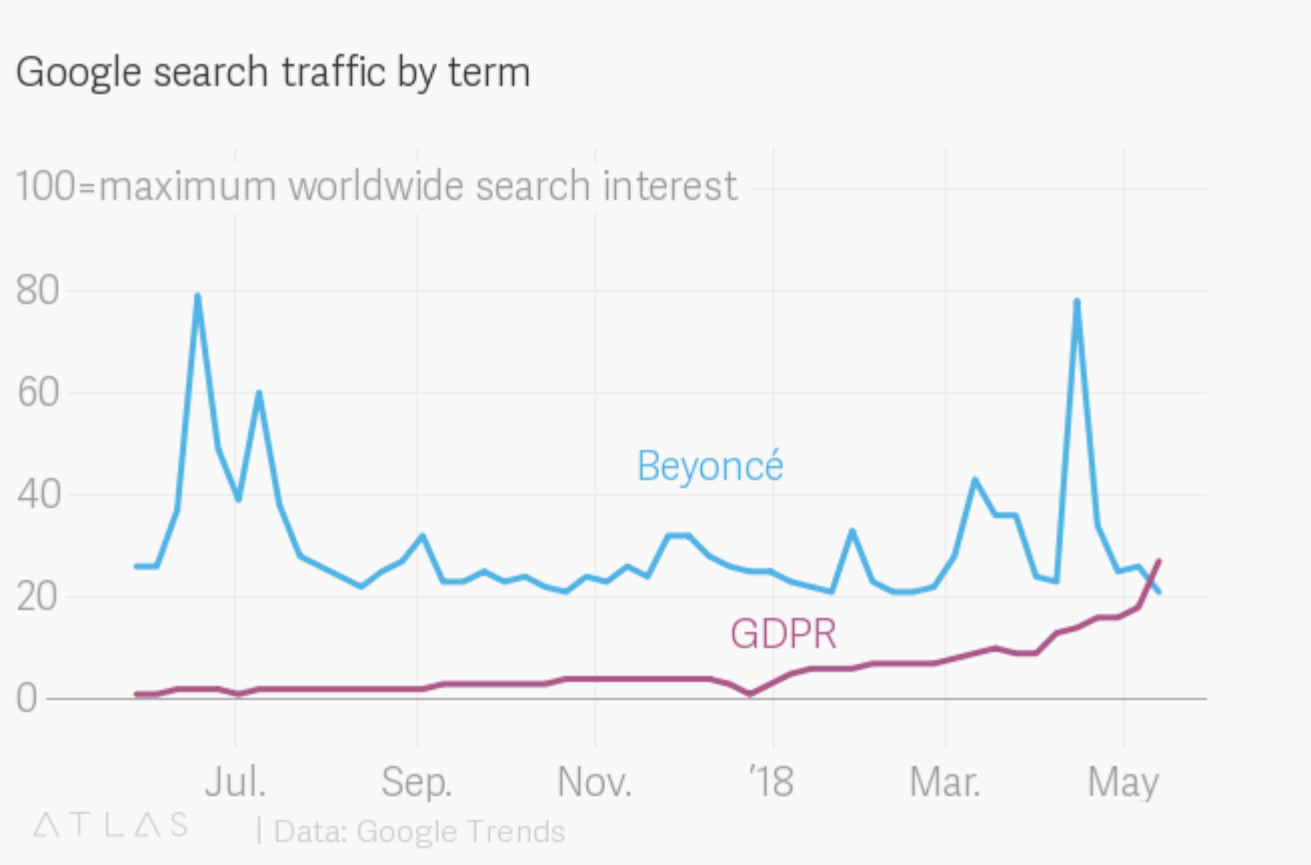
- Data protection impact assessments (DPIAs)
  - DPIAs are a tool to help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy
  - DPIAs must contain:
    - a description of processing operations and purposes, including legitimate interests of the controller (where applicable)
    - an assessment of the necessity and proportionality of processing re purpose
    - an assessment of the risks to individuals
    - measures in place to address risk, including security, and to demonstrate compliance

One year on: what have we learned about the GDPR?

Kelly Fraser

Senior Associate

Despite the hype….



Key developments since the introduction of the GDPR

- Transparency
- Use of consent as a lawful basis
- Use of “legitimate interests” as a lawful basis
- Data sharing
- Data security
- Increased fines
- Effective risk management

Transparency

- Transparency arguably one of the most important data protection principles – firms need to ensure that individuals fully understand how their personal data is used
- Privacy notice is key document to demonstrate compliance with this principle – must be accurate and up to date
- Record of processing activities is also relevant

Consent as a lawful basis

- Under the GDPR, limited circumstances where consent is appropriate
- Consent likely to be inappropriate where:
  - It is a precondition to access services
  - Firm is in a position of power over the individual (such as an employer and employee)
  - Firm would still process the personal data under another lawful basis if consent is refused or withdrawn
- Consent must be freely given, which means that individuals should have a genuine choice over whether or not they give consent
- If a consent request includes a pre-ticked box, this will fall foul of the GDPR's requirements as consent requires a positive action to opt in

“Legitimate interests” lawful basis

- The “legitimate interests” lawful basis applies where it is necessary to process personal data to pursue the controller’s or a third party’s legitimate interests
- However, it only applies where such interests are not overridden by the individual’s interests – for example, where no harm will result to the individual’s rights and freedoms
- To use legitimate interests as a lawful basis to process personal data, a three stage assessment must be undertaken by firms to ensure that this is appropriate. This is called a legitimate interests assessment (“LIA”)
- This is a light touch risk assessment based on the specific circumstances and context of the particular processing

Data sharing

- Different requirements where a firm , as a controller, shares personal data with a processor or another controller
- When sharing personal data with a **processor**, the GDPR requires a contract and prescribes a list of provisions for that contract. As well as ensuring a contract is in place, firm needs to take steps to monitor the processor's compliance with the contract
- When sharing personal data with a **controller**, there are no similar prescriptive provisions within the GDPR and the ICO is currently updating its data sharing code of practice
- The GDPR does provide that where sharing of personal data is between **joint controllers**, an arrangement is required to determine respective responsibilities for compliance

Data security

- Security is a key principle under the GDPR:
  - Risk analysis
  - Organisational policies
  - Physical / Technical measures
- Three elements of information security:
  - **Confidentiality:** unauthorised or accidental disclosure of or access to personal data
  - **Integrity:** unauthorised or accidental alteration to personal data
  - **Availability:** unauthorised or accidental loss of access to, or destruction of, personal data

Data security

- New duty to report certain personal data breaches to:
  - The ICO within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals
  - The affected individuals if a personal data breach is likely to result in a high risk to their rights and freedoms and notification is required by law
- Example of ICO considerations:
  - The number of data subjects affected
  - The type of personal data involved
  - Any risk to the data subject as a result
  - Any processes in place
  - Any remedial steps taken

Increased fines

- Previous £500k cap under the Data Protection Act 1998 increased to 4% of annual worldwide turnover or €20m (whichever is greater) for the most serious personal data breaches under the GDPR
- ICO is still dealing with backlog of breaches but two notable intentions to fine announced:
  - BA cyber fraud incident affecting approximately 500,000 customers: ICO intends to issue fine of £183.39m (1.5% of global annual turnover) and also compensation action raised in the courts with estimated cost of £800m
  - Marriott guest reservation systems compromised on company it acquired: ICO intends to issue fine of £99.2m (3% of global annual turnover)

Creating and implementing an information-aware culture in the workplace

Scott Kerr

Partner

Creating

- The policy
  - Understanding your own business
  - Consultation

- Training
  - For all
  - Ongoing
  - Recorded

Applying

- A DPO?
  - Oversight
  - Shared role

- Security
  - In the office
  - Out the office
  - IT

Policing

- Breaches
  - Common risks
  - Carrot v stick
  - Response

- Reporting
  - ICO
  - Client

Subject Access Requests

- Recognising
- Responding
- Responsibility

Questions

Contact us

Kelly Fraser
Senior Associate
t: +44 (0)141 227 9306
e: kelly.fraser@harpermacleod.co.uk

Scott Kerr
Partner
t: +44 (0)131 247 3336
e: scott.kerr@harpermacleod.co.uk