GDPR – what we have learned so far

Kelly Fraser

29 November 2018

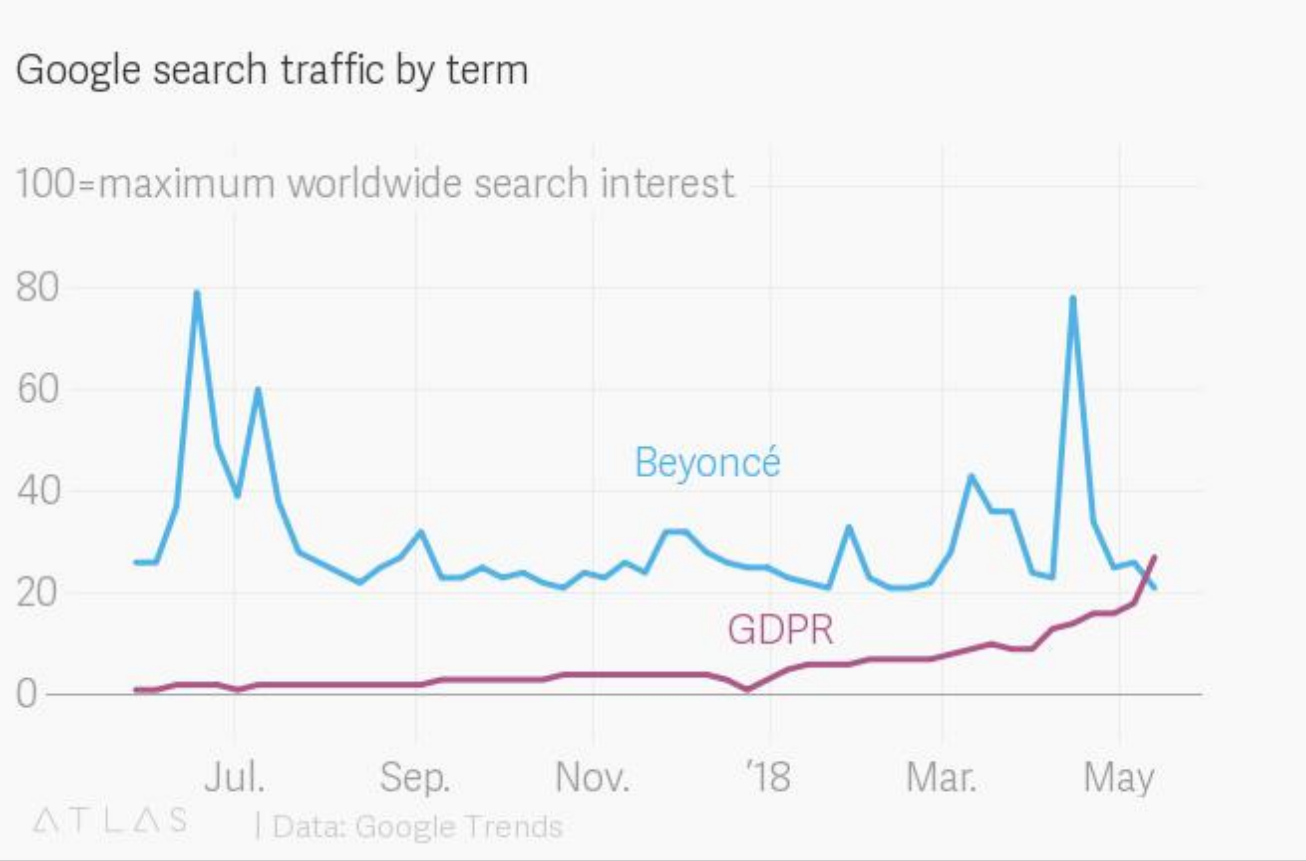
Driven to deliver

Harper Macleod LLP

Overview

1. The legislation
2. Overview of key changes and common pitfalls
3. Data protection by design and default
4. Role of the Data Protection Officer
5. Personal data breaches
6. Offences
7. Key messages
8. Questions

Despite the hype…



Harper Macleod LLP

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

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

The legislation

- The GDPR sets out:
  - Data protection principles (Article 5)
  - Lawful processing (Articles 6 and 9)
  - Rights of data subjects (Articles 13 to 22)
  - Processors (Article 28)
  - Notification of personal data breaches (Articles 33 and 34)
  - Data protection impact assessments (Article 35)
  - Designation of Data Protection Officer (Article 37)
  - International transfers (Articles 44 to 50)

The legislation

- The DPA sets out:
  - Powers of the Information Commissioner (Part 5)
  - Offences (Sections 170 to 173)
  - Conditions for processing special categories or and criminal offence personal data (Schedule 1), subject to ‘appropriate policy document’ requirement (Paragraph 39 of Schedule 1)
  - Restrictions (exemptions) of data subjects’ rights (Schedules 2 to 4)

Overview of key changes and common pitfalls

- 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 compliance include: policies, data protection impact assessments; contracts; and records

Overview of key changes and common pitfalls

- Lawful processing
  - Lawful basis from GDPR list must be identified before processing
  - Consent only applies in limited circumstances
  - Processing of special categories of personal data needs a lawful basis and special condition to be identified before processing takes place
  - 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?

Overview of key changes and common pitfalls

- Data subjects' rights
  - The rights under the GDPR are as follows:
    - Right to be informed
    - Right of access
    - Right to rectification
    - Right to restriction
    - Right to data portability
    - Right to objection
    - Rights re automated decision making and profiling
  - Legal responsibility to identify requests and handle them accordingly
  - Time for responding starts when anyone within firm receives a request

Overview of key changes and common pitfalls

- 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 (Paragraph 5 of Schedule 2)
  - Exemption from data protection principles, right to be informed and right of access re legal professional privilege (Paragraph 19 of Schedule 2)
  - Exemption from data protection principles, right to be informed and right of access re negotiations with data subject (Paragraph 23 of Schedule 2)

Overview of key changes and common pitfalls

- Contracts with processors
  - Processors must be engaged by controllers under written contracts
  - Controllers may only appoint processors which provide sufficient guarantees to implement appropriate technical and organisational measures to ensure processing meets the requirements of the GDPR
  - Monitor compliance with the GDPR and contract
  - Specific provisions re ‘sub-processors’

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
  - Firms with less than 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:
    - Organisation 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 retention policy
  - Law Society guidance regarding client files
  - Other types of personal data will need to be considered and included within policy
  - Risk-based analysis
  - Ongoing compliance

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

Role of the 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 DPIAs
  - 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

Personal data breaches

- 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

Personal data breaches

- Possible personal data breaches include:
  - loss or theft of data or equipment
  - inappropriate access controls allowing unauthorised use
  - equipment failure
  - human error
  - unforeseen circumstances i.e. fire / flood
  - cyber / hacking / server attack
  - blagging offences / fraud
- Robust breach protection, investigation and internal reporting procedures

Personal data breaches

- New duty to report certain personal data breaches to:
  - the ICO within a strict timeframe of 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
- 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

Offence

Harper Macleod LLP

Offences

- Under the DPA it is an offence to:
  - Knowingly or recklessly obtain or disclose personal data without consent of controller; procure disclosure of personal data to another without consent of controller; or retain personal data without consent of person who was controller when it was obtained (Section 170)
  - Knowingly or recklessly re-identify information that is de-identified personal data without consent of controller responsible for de-identifying such data (Sections 171 and 172)
  - Alter, deface, block, erase, destroy or conceal information with intention of preventing disclosure of all or part of information to person make a request under Articles 15 or 20 of the GDPR (Section 173)

Key messages

- Compliance with data protection principles and internal procedures
  - organisational and individual accountability for managing personal data
  - security of personal data, including access
  - data minimisation
  - common sense approach to use of personal data
  - breach reporting
  - data subject rights' requests
  - privacy information

Questions

Harper Macleod LLP

Contact details

Kelly Fraser

Associate

t: +44 (0)141 227 9306

e: kelly.fraser@harpermacleod.co.uk

Harper Macleod LLP