Beale&Company

London | Bristol | Dublin | Dubai

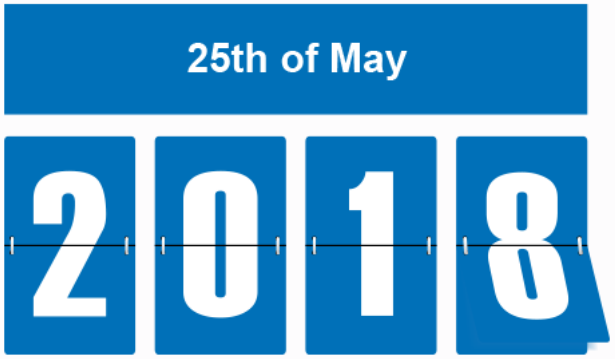
General Data Protection Regulation: An Introduction

James Hutchinson

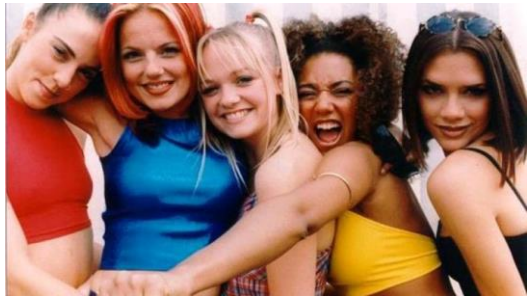
The Chartered Institution of Highways & Transportation – 12 April 2018

Introduction

- General Data Protection Regulation in effect from 25 May 2018
- Probably the most lobbied EU law
- Applies post-Brexit
- One-stop shop for data protection
- Common set of rules applying across the EU
- Direct effect – no need for implementing legislation
- Tougher enforcement and increased penalties
- Significant impact on transport data



Data Protection – 1998 to 2018



Google

facebook

NETFLIX

Overview of GDPR

- Transparency (*Article 5.1*)
  - New obligation of transparency
  - Adds to existing obligations to process fairly and lawfully
- Consent (*Article 7*)
  - GDPR stricter on the use of consent
  - Must be freely given, specific, informed and unambiguous
  - Data controller must be able to demonstrate that data subject gave consent
  - If consent given in writing, request must be clearly distinguishable from rest of document
  - Data subjects have right to withdraw consent at any time
- Consider other grounds to justify processing (*Article 6*)

Provision of information on data

- Data controllers currently required to provide data subjects with fair processing information
- Under GDPR (*Article 12*), all information provided must be:
  - Concise
  - Transparent
  - Intelligible
  - Easily accessible
  - In clear and plain language
- Provide information on the legal basis for processing
- Requires a careful analysis of the data processed and available legal bases
- If sensitive data, specify which condition you are relying on
- If relying on “legitimate interest” condition, explain those interests

Provision of information on data (con'd)

- Data controllers must explain:
  - Source of data
  - Who will receive the personal data
  - How long the data will be stored
  - The rights of the data subject, including subject access, rectification and erasure
  - The right to object to processing for a data subject's "particular situation" (*Article 21.1*)
  - The right to withdraw consent
  - The right to complain to the Information Commissioner
  - The legal basis for the transfer of any data outside the EU

New data rights for data subjects

- New “delete it, freeze it, correct it” package of rights (*Articles 12, 15-21*):
- Data subject access rights broadly similar to existing (Article 15)
- Data controllers must provide:
  - Envisaged period of storage
  - Details of the “delete it, freeze it, correct it” rights
  - Safeguards applied on third country transfers of data
- Current 40 day period replaced with obligation to comply:
  - Without undue delay
  - Within one month
  - Extension of two additional months if necessary
- £10 fee abolished – can charge “a reasonable fee” in limited circumstances

New data rights for data subjects (con'd)

- New "delete it, freeze it, correct it" rights:
  - Right to rectification (*Article 16*)
  - Right to erasure (right to be forgotten) (*Article 17*)
  - Right to restrictions of processing (*Article 18*)
  - Right to data portability (*Article 20*)
  - Right to object to processing (*Article 21*)
  - Right to object to automated individual decision-making, including profiling (*Article 22*)
- In general, rights can be exercised where non-compliance with data protection principles

Data Portability (Article 20)

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services
- It allows them to move, copy or transfer personal data easily from one data controler to another provider in a safe and secure way
- Enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits

Automated decision making - profiling (Article 22)

- GDPR introduces a new definition of "profiling" (*Article 4(4)*)

  "*any form of automated processing of personal data consisting of the use of personal data to evaluate personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements*"

- Article 22 introduces a new right:

  "*not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*"

Demonstrating compliance – protection by design

- Must demonstrate compliance as well as comply (*Article 24.1*)
- GDPR requires implementation of data protection policies
- Data protection by design and by default (*Article 25*):
  - Build in safeguards
  - Minimise data collection
  - Only capture what is necessary for the specific purpose for which it is obtained
- Formal contractual requirements between data controllers and processors (*Article 28*)
- New potential liabilities for data processors to data subjects

Contracts between controllers and processors

- Controller must have a written contract in place when using a processor (Article 28.3)
- Contract is important so that both parties understand their responsibilities and liabilities
- GDPR set outs what needs to be included in the contract
- No standard controller/processor wording at the present
- Controller is liable for their processors' compliance with the GDPR
- Controller must only appoint processors who can provide sufficient guarantees
- Processors must only act on the documented instructions of the controller

Contracts between controllers and processors (con'd)

- Controller responsible for ensuring personal data is processed in accordance with the GDPR
- Applies regardless of whether a processor managed data
- Unless controller can prove that it was "*not in any way responsible for the event giving rise to the damage*", controller liable for any damage caused by non-compliant processing
- Controller may however be able to claim back all or part of the amount of compensation from the processor, to the extent that it is liable
- Processor can now be directly liable to pay compensation where:
  - it has failed to comply with GDPR provisions specifically relating to processors, or
  - where it has acted without the lawful instructions of controller, or against those instructions.

Data Protection Officer

- The role of the data protection officer is to:
  - Advise the data controller on its legal obligations
  - Monitor compliance with the GDPR and with data policies
  - Implement related training
  - Be a point of contact with the Information Commissioner's Office
- Data protection officer is independent with a role similar to an auditor
- Not obligatory to appoint a data protection officer
- EU has published guidance and a set of Frequently Asked Questions about the role of the data protection officer at:

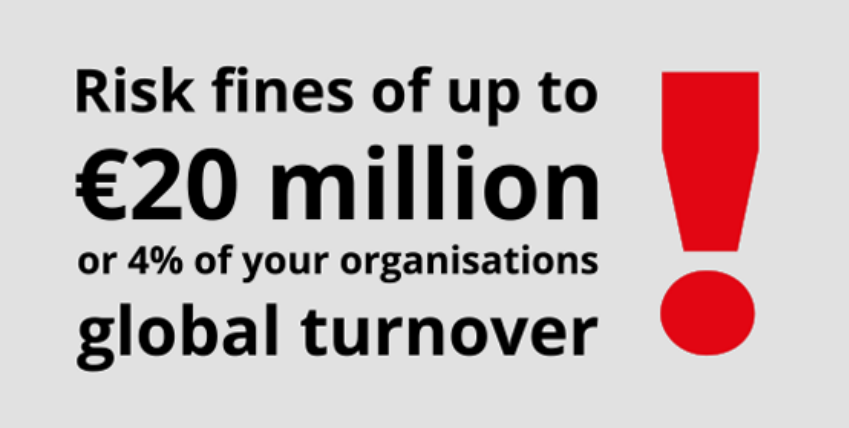
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf

Reporting a breach

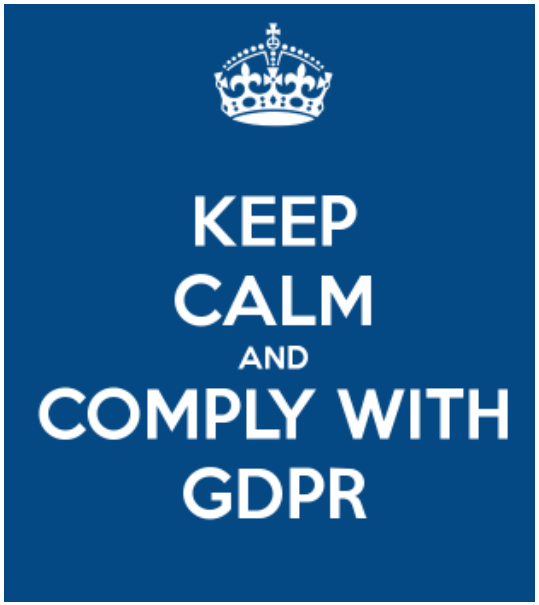
- What is a personal data breach? (*Article 33*)
  - A breach of security
  - Leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data
- Examples – sending emails to wrong person
- On discovery, duty to notify ICO promptly and within 72 hours, if feasible
- Obligation to:
  - Describe what happened
  - Set out approximate number of individuals affected
  - Likely consequences and measures taken or proposed
- If high risk to data subject, they must be told

Insurability of GDPR fines

- Grey area and depends on the particular facts of the claim
- Key question is whether a fine is criminal or quasi criminal – public policy
- Penalties are meant to be punishing
- May be some circumstances where an insured can be indemnified
- Look at precise wording of cyber policies



Just over one month to go – steps to take



- Identify existing data systems and what personal data you process
- Allocate resources to prepare for change
- Review privacy notices and other fair-processing information
- If you rely on consent for processing, consider other routes
- Review policies, contracts with data processors, suppliers
- Review data breach policy
- Train staff on GDPR requirements
- Develop and implement policy of retention and storage of data

Resources

- Text of the General Data Protection Regulation ((EU) 2016/679) - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
- Overview of the GDPR - https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- General Guidance from the Information Commissioner - https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/
- Preparing for the General Data Protection Regulation (GDPR) – 12 Steps to Take Now - https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf
- ICO Guidance - Contracts and liabilities between controllers and processors - https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

Questions

James Hutchinson
Partner

Tel: +44 (0) 20 7469 0408
Email: j.hutchinson@beale-law.com
Web: www.beale-law.com
Twitter: @cyberclaims