General Data Protection Regulation: Preparation for Employers

James Hutchinson
2 August 2017
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 employee data
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
  - Employer must be able to demonstrate that employee gave consent
  - If consent given in writing, request must be clearly distinguishable from rest of document
  - Employee has right to withdraw consent at any time

+ Consider other grounds to justify processing (*Article 6*)
Provision of information on data

+ Employers currently required to provide employees 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 (continued)

Employers must explain:

- Source of data
- Who will receive the personal data
- How long the data will be stored
- The right’s of the data subject, including subject access, rectification and erasure
- The right to object to processing for an employee’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 employees

+ New “delete it, freeze it, correct it” package of rights (*Articles 12, 15-21*):
+ Data subject access rights broadly similar to existing (Article 15)
+ Employers 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 employees (continued)

+ 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 object to processing (*Article 21*)

+ In general, rights can be exercised where non-compliance with data protection principles
Employer’s duties

- Employer 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
- Role of the Data Protection Officer
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, loss of hard drive
+ 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
  – Measures taken or proposed
+ If high risk to data subject, they must be told
One year to go – steps to take now

- Identify existing data systems and what personal data you process
- Allocate resources to prepare for change
- Consider appointing a Data Protection Officer (if not mandatory)
- Review privacy notices and other fair-processing information
- If business relies on consent for processing, consider other routes
- Review contracts of employment, policies etc
- Put in place a data breach policy
- Train staff on GDPR requirements
- Develop and implement policy of retention and storage of data
Resources

Thank you

James Hutchinson
Partner

Tel: +44 (0) 20 7469 0400
Email: j.hutchinson@beale-law.com
Web: www.beale-law.com