RUSSELL-COOKE | SOLICITORS

A short introduction to the GDPR

24 April 2018

Victoria Ehmann, Associate

@RCcharityteam

Data Protection – the law

- Now
  - **Data Protection Act 1998** (DPA)
  - **Privacy and Electronic Communications Regulations 2003** (PECR) additional restrictions on direct marketing by electronic means (email, text, internet messaging, telephone)
- 25 May 2018
  - **General Data Protection Regulation** (GDPR) – replace the DPA
  - **Data Protection Bill** – implements EU Law Enforcement Directive and extends data protection laws to areas not covered by GDPR
- Beyond
  - **European Union (Withdrawal) Bill** – will transpose the GDPR into UK law

Who does the GDPR apply to?

- **Data controller** – person or body which determines the purposes and means of processing personal data
- **Data processor** – person or body which processes data on behalf of a data controller (but not data controller's staff)
- **Data subject** – any living, identifiable individual about whom personal data is processed
  - employees, consultants, volunteers, trustees
  - members, parents, contacts at organisations (colleges, universities, museums etc.), contractors, suppliers
  - individuals on contact lists, e.g. fundraising/marketing

What does the GDPR apply to?

- **Personal data** – any information relating to a living person who is identified (or can be identified) from that information
- **Special categories of personal data** (sensitive personal data)
  - race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetics, biometrics (where used for ID purposes);
- Specific rules and guidance concerning **children's personal data**
  - marketing to children, children and consent, rights etc.

Lawful processing (Art. 6 GDPR)

- Identify legal basis for processing personal data:
  - **Consent**
  - Necessary for the **performance of a contract**
  - Necessary for **compliance with a legal obligation**
  - **Vital interests**
  - Necessary to perform a task in the **public interest**
  - Necessary for your **legitimate interests** (or a third party) unless interests override the individual's rights or freedoms

Processing Special Categories (Art. 9 GDPR)

- *Additional* conditions for processing special category personal data include:
  - **Explicit consent**
  - Necessary for carrying out **obligations under employment**, **social security** or **social protection** law
  - **Vital interests**
  - Personal **data made public** by the data subject
  - Necessary for reasons of **substantial public interest**

GDPR consent – what's changing?

- **GDPR** definition
  - **freely given**, **specific**, **informed** and **unambiguous** indication of the data subject's wishes
  - by a **statement** or by a **clear affirmative action**
  - signifying agreement to the processing of personal data relating to him/her
- Must be verifiable – **keep records** of how and when consent was given
- Specific conditions for **consent from children** in relation to online services (Art. 8 GDPR)

Conditions for consent – Art. 7 GDPR

- Written consent:
  - Must be in an **intelligible** and **easily accessible** form
  - Must use **clear** an **unambiguous** language
  - If written document contains other matters (e.g. contract of employment), the request must be **clearly distinguishable from other matters**
- Individual has the **right to withdraw consent at any time** and should be informed of this right before giving consent
  - Must be as easy to withdraw as to give consent

Key concepts – a new approach?

- **Transparency** and **accountability**
  - Data controller will be **responsible for**, and must be able to **demonstrate compliance** with, the principles relating to processing of personal data
- **Record keeping** – some exceptions for organisations with <250 employees
- **Privacy by design and default** (e.g. data minimisation, pseudonymisation, anonymisation, creating and improving security features)
- **Data Protection Officers** and **Data Protection Impact Assessments** (DPIAs)

Individuals' right to be informed

- Data controller must provide privacy information at the time personal data are obtained (free of charge)
- Privacy notice/statement – must include:
  - **Identity** and contact details of **data controller**
  - Contact details of data protection officer (where applicable)
  - **Purposes** of intended processing and legal basis (if legitimate interest, provide information)
  - **Recipient(s)** of personal data
  - Transfer to third country or international organisation (where applicable)

Privacy Notices – Art. 13 GDPR

- In addition:
  - **Period data will be stored** or (if not possible) criteria used to determine period
  - Right to request **access** data, to **rectification** or **erasure**, right to **restriction** of processing, right to **data portability**
  - If consent relied upon, **right to withdraw consent** at any time
  - **Right to lodge complaint** with ICO
  - Whether there is a **statutory or contractual requirement**
  - Any **automated decision-making** (including profiling)

Retention and deletion of data

- No specific time – statutory requirements
  - E.g. tax, health and safety, charity law, safeguarding, regulatory requirements…
- **Establish** and **adhere to** standard retention times for category of information being held
  - E.g. data about a job applicant - ICO Employment Practices Code says recruitment data should not be kept for more than 6 months in most cases)
- Ensure records to be disposed of are securely and effectively destroyed when **no longer required** to fulfil the **purposes for which they were originally collected**

GDPR – rights of individuals

- Right to be **informed** (transparency) **–** privacy notices
- Right of **access –** subject access requests
- Right to **rectification –** if data is inaccurate or incomplete
- Right to **erasure –** 'right to be forgotten'
- Right to **restrict processing –** storage only
- Right to **data portability –** moving data from one IT environment to another
- Right to **object –** includes absolute right to object to direct marketing
- Rights re: **automated decision making** and **profiling**

Third-Party Data Processors

- Art. 28 – only use processors providing "**sufficient guarantees**" that processing will meet GDPR requirements and ensure protection of individual rights
- Processing by data processor must be governed by a contract with the data controller, to include:
  - subject-matter and duration of processing
  - nature and purpose of processing
  - type of personal data and categories of data subjects
  - obligations and rights of the controller

ICO – notification of breach

- GDPR Art. 33 – requirement for data controller to **notify a personal data breach to ICO** as the supervisory authority
  - Only if breach likely to result in risk to rights and freedoms of individuals
  - Without undue delay
  - Where feasible, not later than 72 hours after becoming aware of it
- If data breach **likely to result in high risk to rights and freedoms** of an individual, controller must also **communicate the breach to the individual** without undue delay

Contact

Victoria Ehmann
Associate
T: +44 (0)20 8394 6464
Victoria.ehmann@russell-cooke.co.uk

Russell-Cooke is a top 100 firm with around 200 highly regarded specialist solicitors and lawyers. We advise a mix of commercial and not-for-profit clients.