Preparing for GDPR:

set your organisation on the path to compliance

10 October 2017

adapta

RUSSELL-COOKE | SOLICITORS

Introduction

09.20 **The legal perspective – overview of legal requirements**

09.45 **Practical considerations for responding to the GDPR**

10.10 **Group work: demystifying the requirements GDPR**

10.40 Short coffee break

10.55 **Follow-up to group work/case studies**

11.40 **Developing an action plan**

12.00 **Practical next actions**

12.30 **Summary and close**

adapta

RUSSELL-COOKE | SOLICITORS

RUSSELL-COOKE | SOLICITORS

The legal perspective

An overview of legal requirements highlighting what's new in the GDPR

Data Protection – the current law

- **Data Protection Act 1998** (DPA)
- **Privacy and Electronic Communications Regulations 2003 (PECR)** additional restrictions on direct marketing by electronic means (phone, fax, email, text, video messaging), rules on cookies etc.
- **Regulation of Investigatory Powers Act 2000 (RIPA)** covers 'interception' of communications (e.g. monitoring employee emails or internet usage)

Data Protection – the new law

- **General Data Protection Regulation** (GDPR) – replace the DPA from 25 May 2018
- **Data Protection Bill** – will repeal DPA and incorporate GDPR once UK leaves EU
  - continuity of data protection standards in the UK following Brexit
  - UK derogations – national laws permitted by the GDPR in specific contexts

Who does the GDPR apply to?

- **Data controllers**
  - person or body which determines the purposes and means of processing personal data
- Can have joint data controllers
- Broadly same as DPA
- GDPR extends obligations and potential liability to **data processors**
  - person or body which processes data on behalf of a data controller (but not data controller's staff)

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 - Art. 5(2) GDPR
- **Governance**
  - ICO expects “comprehensive but proportionate” governance measures”
  - Privacy by design and default (e.g. data minimisation, pseudonymisation, creating and improving security features on an ongoing basis)

Governance

- Appropriate **technical and organisational measures**
- **Documentation** – requirement to keep records of processing activities
- Requirement for some organisations to appoint a **Data Protection Officer (DPO)**
- Compulsory **Data Protection Impact Assessment (DPIA)**

Key definitions

- **Personal data**
  - information relating to a living person who is identified (or can be identified) from that information
- **Special categories of personal data** – (DPA 'sensitive personal data')
  - personal data revealing race or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation

Data Protection Principles (Art. 5 GDPR)

- Personal data must be:
  - processed **lawfully**, **fairly** and in a **transparent** manner
  - Collected for **specified**, **explicit**, and **legitimate** purposes and not be processed in a way that is incompatible with those purpose(s)
  - **adequate**, **relevant** and **limited to what is necessary** in relation to the purpose(s) for which it is processed
  - be **accurate** and, where necessary, **kept up to date**

Data Protection Principles (Art. 5 GDPR)

- kept for **no longer than is necessary** for the purposes for which the data are processed
- processed in a manner that ensures **appropriate security** of the data (including to prevent unauthorised or unlawful processing, accidental loss, destruction or damage) using appropriate **technical or organisational measures**
- must **not be transferred outside the EEA** unless the country has an adequate level of protection for data subjects

Lawful processing (Art. 6 GDPR)

- Identify and record legal basis for processing personal data:
  - **Consent** of data subject
  - Necessary for the **performance of a contract** or to take steps to enter into a contract with data subject
  - Necessary for **compliance with a legal obligation**
  - Necessary **to protect the vital interests** of a data subject or another person
  - Necessary for the performance of a task carried out in the **public interest** or in the exercise of **official authority**
  - Necessary for the purposes of **legitimate interests** pursued by the data controller or a third party

Processing Special Categories (Art. 9 GDPR)

- Conditions for lawfully processing special categories of personal data include:
  - **Explicit consent** (opt-in)
  - Necessary for carrying out **obligations under employment**, **social security** or **social protection** law, or a collective agreement
  - Necessary **to protect the vital interests** of the data subject
  - **Provision of health or social care or treatment** or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

Consent - GDPR

- 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
- Verifiable – **keep records** of how and when given
- Specific conditions for consent if providing online services to children under 13

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

Consent – ICO draft guidance

- ICO draft guidance
  - *Consent requires an active opt-in – unticked opt-in boxes or similar active opt-in methods (e.g. yes/no)*
  - *Be specific and granular – vague or blanket consent not appropriate*
  - *Name any third parties who will rely on the consent*
  - *Keep your consent requests separate from other terms and conditions*
  - *Avoid making consent a precondition of a service*

Privacy Notices – Art. 13 GDPR

- Controller must provide at the time personal data are obtained (free of charge)
- Notice 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)

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 right to object to direct marketing
- Rights re: **automated decision making** and **profiling**

Right of Access

- Subject Access Requests under DPA – what will change?
- Must provide copy of information **free of charge** – can charge ‘reasonable fee’ if request manifestly unfounded or excessive
- **1 month** (at the latest) to comply – can be extended where requests are complex or numerous
- If request made electronically, provide information in a commonly used **electronic format**
- Wherever possible, provide **remote access** to secure self-service system

Right to Object

- Individuals have the right to object to:
  - processing based on **legitimate interests** or performance of a task in the public interest/exercise of official authority
  - **direct marketing** (including profiling)
  - processing for purposes of scientific/historical research and statistics
- Legitimate interests – stop processing **unless** compelling legitimate grounds or legal claims

Right to Erasure

- Known as '**right to be forgotten**' – right to request deletion or removal of personal data, e.g.
  - personal data no longer necessary in relation to purpose it was originally collected/processed
  - individual withdraws consent or objects and no legitimate interest for continuing processing
- **Refusing** request for erasure, e.g.
  - to comply with a legal obligation for the performance of a public interest task or exercise of official authority
  - for public health purposes in the public interest
  - exercise or defence of legal claims

Third-Party Data Processors

- Art. 28 – controller must 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 written **contract** with the data controller
- Controllers and processors must maintain a **record of processing activity** carried out

ICO breach notification

- 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

ICO Powers – Art. 58 GDPR

- **Investigative powers**, including:
  - Order controller and processor to provide information
  - Data protection audits
  - Entry, inspection and seizure (documents and equipment)
- **Corrective powers**, including:
  - Warnings, reprimands and orders for compliance
  - Temporary or definitive ban on processing
  - Order the rectification or erasure of personal data or restriction of processing

ICO Powers – Penalties and Fines

- Art. 83 GDPR graduated fines depending of type and severity of infringement - must be effective, proportionate and dissuasive
- Depending on breach:
  - <EUR10 million or <2% of total worldwide annual turnover, whichever is higher
  - <EUR20 million or <4% of total worldwide annual turnover, whichever is higher
- Reputational damage (media interest) and/or potential action by charity commission

Contact

Carla Whalen
Associate Qualified in Scotland
T: +44 (0)20 8394 6419
carla.whalen@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.

Practical considerations for responding to the challenges of GDPR

Fiona Brookes, Adapta Consulting

adapta

Practical steps for achieving GDPR compliance

1. Appoint a DPO / DP lead

2. Raise awareness & provide training

3. Undertake a compliance review – process & systems

4. Document your data handling processes

5. Determine & document your lawful basis for processing

6. Determine & implement your consent strategy

7. Develop a personal information register

8. Revise & develop your data protection compliance policies, procedures

9. Embed privacy by design & impact assessments

10. Move to full channel specific opt-ins for DM communications

11. Issue & collect revised data processor agreements

12. Develop & implement a plan for ongoing compliance

adapta

Group work:
demystifying the requirements GDPR

Russell Cooke

adapta

RUSSELL-COOKE | SOLICITORS

Group work:
demystifying the requirements GDPR

Follow-up to questions/group presentations

Russell Cooke

adapta

RUSSELL-COOKE | SOLICITORS

Developing an action plan

Adapta consulting
Russell Cooke

adapta

RUSSELL-COOKE | SOLICITORS

Practical next steps

Russell Cooke

adapta

RUSSELL-COOKE | SOLICITORS

Summary and close

Adapta Consulting
Russell Cooke

Presentations will be available online shortly

adapta

RUSSELL-COOKE | SOLICITORS