GDPR

Briefing to HR Senior Advisers Team on the new General Data Protection Regulation

Seeq Nong, Privacy Adviser

21 April 2016

EVERY JOURNEY MATTERS

What is this new law?

The General Data Protection Regulation (GDPR) was approved by the European Parliament on Thursday 14 April 2016 after four years of negotiations. It is expected to be in force in May 2016 and will be fully implemented by the summer of 2018.

The GDPR will replace the current Data Protection Act 1998.

What are the key changes?

There are significant changes introduced and below are just a few of the key changes:-

- Fines of up to 4% of annual turnover (or €20,000,000) for serious breaches of the GDPR! This is a huge deterrent to breaking the rules;
- Personal data breach notification – Data controllers must notify the supervisory authority (Information Commissioners Office) 'without undue delay' or within 72 hours of being made aware that personal data has been lost; if there is a high risk to individuals then they must be informed;
- Expanded scope – applies to **all data controllers and processors** (service providers) **established in the EU** and organisations that target EU citizens;
- New obligations on data processors – they become an officially regulated entity;
- Consent – must be 'freely given, specific, informed and unambiguous; explicit consent for processing sensitive personal data;
- Accountability – obligations include: documenting data processing activities, policies; building in data protection safeguards in new systems or processes, including privacy friendly default settings (set at highest level) on for example, social networks and apps;
- Privacy Impact Assessments;
- ***New*** enhanced rights - substantial rights given to data subjects including:
    - ✓ Right to be forgotten
    - ✓ Data portability rights
    - ✓ Right to object to profiling - right not to be subject to decisions based solely on automated processing

Changes to Subject Access Requests (SARs)

1) Will have just a month to process (instead of 40 days)

2) Free (can no longer charge £10 although can charge a reasonable amount to meet administrative costs if extra copies of information is requested)

3) Exemptions not to comply – manifestly unreasonable **or** excessive requests can be charged or refused

4) When supplying the information, must also provide the following:-

   - ✓ Purpose of processing (e.g staff administration)
   - ✓ Categories of data processed
   - ✓ Exemptions (if withholding or redacting information)
   - ✓ Description of the source of the information (e.g individuals data subjects have named on their request and DA)
   - ✓ Any regulated automated decision making
   - ✓ Right to lodge complaint to the ICO
   - ✓ Data retention period
   - ✓ Right to have inaccurate data corrected
   - ✓ Right to object to processing,
   - ✓ Who the information is shared with (eg international organisations or countries outside the EU)

SAR Complaints

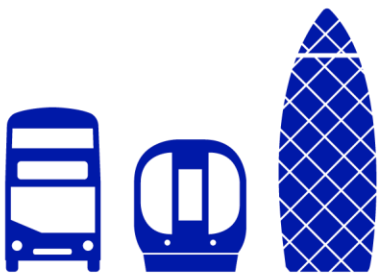
Reasons:

1. Response times exceed 40 calendar days
2. Response doesn't include all data which the requester believes should exist and should have access to this
3. Data provided has been excessively redacted
4. Requester unable to access information where provided in electronic form

Potential consequences of not complying with SARs:

ICO investigation which can lead to:

- Fines
- Enforcement notice (is a criminal offence to ignore these)
- Undertaking
- Inspection and audit
- Prosecution – corporate or individual
- Reputational damage – ICO findings are often published, loss of confidence by customers
- Data subjects can take own legal action



Action taken by the ICO relating to SARs

Enforcement:

MI Wealth Management Company – 18 March 2016: Failure to comply with a SAR

Wainwright Estate Agents – 03 March 2016: Failure to comply with SAR

Undertaking:

Pembrokeshire County Council – June 2015: This follows an incident where sensitive personal data relating to a number of individuals was not properly redacted from a response to a subject access request. Procedures were in place but there was a lack of oversight of the request.

Advisory Visit:

NI Prisoner Ombudsman – January 2015: ICO invited to provide advice and guidance on keeping personal secure and dealing with SARs.