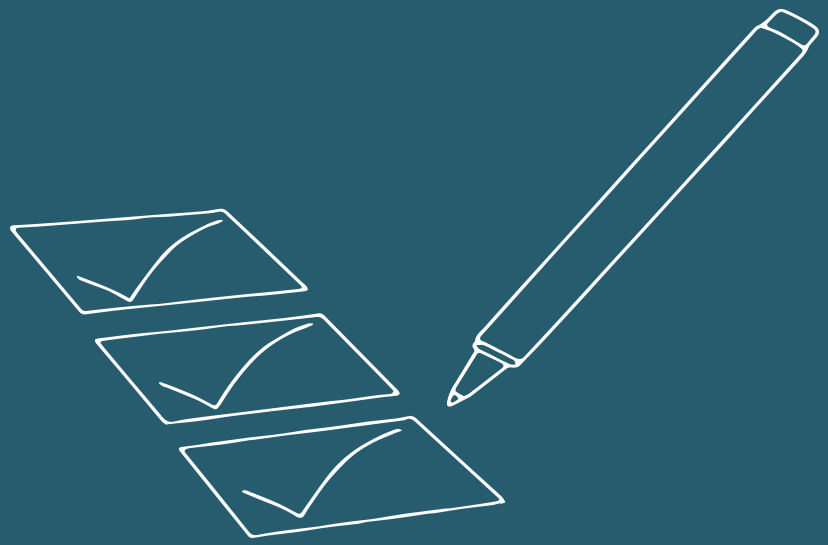
The General Data Protection Regulation

Presentation for The House: December 2017



Thomson Snell & Passmore

The General Data Protection Regulation

What is the GDPR?

- An EU Regulation with direct effect as law in UK
- Comes into force on 25 May 2018
- Strengthening previous laws and introducing new requirements
- Will continue to apply regardless of UK leaving the EU

The General Data Protection Regulation

Does GDPR affect your organisation?

GDPR applies to:

- Data controllers and data processors in the UK and EU
- Non-EU Data controllers and processors targeting UK and EU citizens

Principles of processing personal data

Personal data must be:

- **Processed lawfully**, fairly, in a transparent manner
- Collected for specified, explicit and **legitimate purposes**
- Adequate, **relevant**, and limited to what is necessary
- Accurate and, where necessary, kept up-to-date
- **Kept for no longer than is necessary** for the legitimate purpose
- Processed using adequate security (appropriate tech/org measures to prevent unlawful access/loss or damage)

The General Data Protection Regulation

The Fines

Both data controllers and data processors can be fined for GDPR breaches:

Lower level breaches

Higher of:

- Up to €10,000,000; or
- Up to 2% of the total worldwide turnover (previous year)

Higher level breaches

Higher of:

- Up to €20,000,000; or
- Up to 4% of the total worldwide turnover (previous year)

How to start planning for GDPR

Step 1: Carry out a data audit

- What types of personal data do you hold?
- Who processes it?
- Where did it come from?
- Is it shared with 3rd parties?
- What is your legal basis for collecting/holding the personal data?
- If consent, do you have a record of this?
- Was the personal data collected in accordance with your data privacy policies?
- Review your security procedures for storing personal data
- Review whether your current retention scope & periods are appropriate
- Understand how you destroy personal data

The General Data Protection Regulation

Step 2: Understand your legal bases for processing personal data

- **Consent:** the individual has given you consent to process his/her personal data
- **Contracts with the individual:** for the performance of a contract. (For example: fulfilling services or employment contract)
- **Compliance with a legal obligation:** if the processing is required by UK or EU law
- **Vital interests:** processing to protect the data subject's life or someone else's life
- **Public tasks:** processing to fulfil official functions/perform public interest tasks (UK public authorities)
- **Legitimate interests:** if you have a genuine legitimate reason, including commercial benefit, to process the personal data. (However, the processing should not have an unwarranted impact on data subjects, and it should still be fair, transparent and require accountability.)

Step 3: Check you have valid consent, where required

Under the GDPR, consent must be:

- freely given
- specific
- informed
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Higher compliance standard than DPA! It's important to review and update (if necessary) how you obtain, record and manage your requests for consent

Additional points about consent

- What does explicit consent mean in relation to sensitive personal data?
- How long does any form of consent last?
- Who can give consent?
- How should you write a consent request?
- How should you record consent?

The General Data Protection Regulation

Methods to obtain consent

The ICO suggests the following methods would be GDPR compliant indications of the individual's consent:

- signing a consent statement;
- ticking an opt-in box on paper or electronically;
- clicking an opt-in button or link online;
- selecting 'yes' or 'no' options;
- choosing technical settings or preference dashboards settings;
- responding to an email requesting consent;
- answering "yes" orally; and
- "just in time" notices (these appear on-screen at the point the person inputs data, with a brief message about what the data will be used for).

NB: The following would not constitute valid consent: silence; inactivity; pre-ticked boxes; opt-out boxes

When would consent be inappropriate?

Don't use consent as a basis for processing if you cannot offer a genuine choice over how you use their data: For example:

- If you would still process the data using a different lawful basis if consent was refused or withdrawn.
- If you would ask for consent to the processing as a precondition of accessing services.
- You are in a position of power over the individual.

The right to withdraw

In your request for consent, you must include information about how individuals can withdraw their consent.

They must be able to withdraw consent without suffering detriment, and it must be **as easy to withdraw consent as it is to give it**. It should be **easily accessible** and a **one-step** process.

Upon receipt of the withdrawal of consent, you should stop processing the data immediately.

Accountability & governance

Records of processing activities

If your organisation has >250 employees, keep records of:

- Name and details of your organisation;
- Purposes of the processing;
- Description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Details of transfers to other countries including documentation of the transfer mechanism safeguards in place;
- Retention schedules; and
- Description of technical and organisation security measures taken

If your organisation has <250 employees, it is still a good idea to keep the above records!

Organisations of **any size** are required to maintain records of activities related to higher risk processing such as those relating to special categories of data (sensitive personal data) and those that could jeopardise the rights and liberty of individuals.

Data protection officer (DPO)

Data Controllers and Processors must appoint a Data Protection Officer (DPO) where they:

- Are a public authority/body
- Have core activities requiring large scale ‘systematic monitoring’ of individuals
- Have core activities requiring large scale processing of special categories of data

If DPO not strictly required for your organisation – consider appointing one anyway!

What is the DPO's role?

The DPO must:

- Be able to perform the role **independently**.
- Be capable of reporting to the highest management level;
- Be **point of contact** for supervisory authorities and data subjects contact DPO directly;
- Have professional **experience & expert knowledge** of DP law/practices;
- Keep up-to-date on the obligations to comply with data protection laws + keep the organisation and other employees informed;
- **Monitor compliance**, advise on data protection impact assessments, conduct internal audits; and
- Be given required resources – senior management, HR, IT & Legal support, time to do job, staff and training.

The General Data Protection Regulation

Third parties and outsourcing

- If data processing is outsourced (e.g. payroll administration, internet service providers) make sure the third party provider complies with data protection laws

- You (the data controller) must enter into a written contract with the data processor which requires them to:

  – act only on your instructions;

  – limits their use of the personal data; and

  – imposes security measures matching the data controller's obligations

Transferring data outside the EU

You may transfer personal data to a non-EU country or international organisation if:

1. **Commission has issued an adequacy decision** (i.e. that the organisation, country, territory or sector ensures adequate levels of protection);

2. **The organisation has adequate safeguards**;

3. **Derogation is permitted by the GDPR**

   If an **adequacy decision** or **adequate safeguards** don't apply, there are some special exemptions (derogations) from the general prohibition on transfers of personal data.

Privacy Impact Assessment

PIAs are tools to help organisations be compliant. PIAs were previously only encouraged under the DPA, but GDPR requires them when ***using new technologies*** or when ***data processing is likely to result in a high risk to individual's rights and freedoms***.

The PIA should cover:

- What is the activity meant to achieve?
- What risks does the activity pose?
- Could the objective be achieved without sharing or processing personal data?

Breach notification

"A breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."

- Internal procedures must be put in place covering the PROMPT detection, investigation and reporting of breaches.

- You must notify the ICO of a breach where it is likely to result in a risk to individuals' rights and freedoms (e.g. potential reputational damage, financial loss, discrimination, loss of confidentiality, etc.)

- This must be done within **72 hours** of your organisation becoming aware of the breach unless the data breach is likely to result in a high risk to the rights and freedoms of individuals, in which case you must inform them ASAP.

Failure to notify a breach when required to do so can result in a fine (up to €10million or 2% of global annual turnover).

The General Data Protection Regulation

Compliance with individuals' rights

Individuals have a number of continuing rights to their data under the GDPR:

- the right to be informed
- the right of access
- the right to rectification
- the right of erasure
- the right to restrict processing
- the right to data portability
- the right to object
- rights re automated decision making and profiling

The General Data Protection Regulation

Data protection in the HR context

- Personal data in the employee content will include:
  - names
  - emails
  - salary/expenses
  - employment records
  - occupational health records
  - photographs

- Less obvious but also included:
  - browsing history
  - on-line data
  - analytics
  - cookies
  - OBA
  - CCTV
  - criminal record check information (NB: prohibition on any collection or processing of criminal records, except as authorised by law/regulation)

- Your processing of employee personal data will generally be on the basis of fulfilling an employment contract but this doesn't alter your obligations to deal with that data in accordance with the data protection principles!

Contact us

Gina Bicknell
Partner
01892 701279
gina.bicknell@ts-p.co.uk

Stuart Smith
Consultant
07827 962669
Stuart.smith@ts-p.co.uk

Where we are based:

Tunbridge Wells
3 Lonsdale Gardens
Tunbridge Wells
Kent TN1 1NX

Thames Gateway
Corinthian House
Galleon Boulevard
Crossways Business Park
Dartford
Kent DA2 6QE

@pragmaticlawyer

Last updated September 2017