General Data Protection Regulation (GDPR): What You Need to Know

13 April 2018

Impact of GDPR

- **An organisation that holds personal data needs to comply with GDPR**
- **Accountable to the Information Commissioner's Office ("ICO")**
- **Accountability is not a new requirement.**
- **GDPR requires all organisations to record and document compliance with all applicable aspects of GDPR, the regulation gives individuals more rights in respect of their data: including more control and visibility of how their personal data is being used, and the right to have that information removed or moved if requested.**

Compliance with GDPR

- **Undertake data mapping to understand your data sources and storage for all stages of data custody.**
- **Look to identify what you are doing with data, how you are protecting data and how we are ensuring we do not infringe on the rights of the subject of that data. That includes that personal data should be obtained for one or more specified purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.**
- **Understanding our data uses for the specific purposes for which the data is being collected (legitimate interests, records of processing, consent, ensuring that data is adequate, relevant and not excessive in relation to the purpose).**

Compliance with GDPR

- **Protecting the individual – the right to be informed; the right of access; the right of rectification; the right of erasure; the right to restrict processing; the right to data portability; the right to object and rights in relation to automated decision making and profiling.**

- **Implementing appropriate technical and organisational measures to protect data against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**

- **Implementing appropriate controls to avoid that data is transferred to a country or territory outside the European economic area unless that country or territory ensures that an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.**

Policy

- **Processed lawfully, fairly and in a transparent manner in accordance with the General Data Protection Regulation (the "GDPR") given the purposes for which those data were obtained;**
- **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;**
- **Adequate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;**

Policy

- **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;**

- **Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.**

Personal Data

- **Any information relating to an identified or identifiable natural person;**
  - **an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**

Personal Data Includes:

- **Personnel records;**
- **Customer details;**
- **Sales and Marketing;**
- **Prospect information;**
- **Online identifier data etc.**

Awareness and Communication

- People within your organisation should be aware of GDPR
- Appreciate the impact this is likely to have and identify areas of potential compliance problems
- Review the risk register
- Plan for implementation.

Data Mapping

- What personal data do we hold?
- Where did it come from?
- Who do we share it with?
- In what format do we hold it?

Privacy Information

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

Privacy Information

- **It must be concise, transparent, intelligible and easily accessible;**
- **Written in clear and plain language, particularly if addressed to a child; and**
- **Free of charge.**

Data Controllers and Data Processors

- **GDPR applies to controllers and processors;**
  - **A controller determines the purposes and means of processing personal data**
  - **A processor is responsible for processing personal data on behalf of a controller**

- **If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.**

- **If you are a controller, you are not relieved of your obligations where a processor is involved. The GDPR places further obligations on you to ensure your contracts with processors comply with GDPR.**

Data Controller

- **Shall be responsible for, and be able to demonstrate, compliance with the principles.**

Data Processor

- Review the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity
- Check that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.
- Record our decision on which lawful basis applies to help us demonstrate compliance.
- Include information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.
- If process special category data, also identify a condition for processing special category data, and have document this.

Data Protection Principles

Personal data shall be:

- **Processed lawfully, fairly and in a transparent manner in relation to individuals;**
- **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;**
- **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;**

Data Protection Principles

- **Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;**
- **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and**
- **Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.**

Lawful Basis for Process

- **Consent: the individual has given clear consent for you to process their personal data for a specific purpose.**
- **Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.**
- **Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).**

Lawful Basis for Process

- **Vital interests: the processing is necessary to protect someone's life.**
- **Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.**
- **Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party.**

Consent

- Make the request for consent prominent and separate from our terms and conditions.
- Ask people to positively opt in.
- Do not use pre-ticked boxes or any other type of default consent.
- Use clear, plain language that is easy to understand.
- Specify why we want the data and what we are going to do with it.
- Give individual (‘granular’) options to consent separately to different purposes and types of processing

Consent

- **Name our organisation and any third party controllers who will be relying on the consent.**
- **Tell individuals they can withdraw their consent.**
- **Ensure that individuals can refuse to consent without detriment.**
- **Avoid making consent a precondition of a service.**
- **If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental consent measures for younger children) in place.**

Recording Consent

- **Keep a record of when and how we obtained consent from the individual**
- **Keep a record of exactly what they were informed at the time.**

Individual Rights

- **Right to be informed;**
- **Right of access;**
- **Right to rectification;**
- **Right to erasure;**
- **Right to restrict processing;**
- **Right to data portability;**
- **Right to object; and**
- **Right not to be subject to automated decision-making including profiling.**

Subject Access Requests

- A month to comply rather than 40 days
- Can refuse or charge for requests that are manifestly unfounded or excessive
- If you refuse you must tell the individual why and that they have a right to complain to the supervisory authority.

Data Breaches

- Have the right procedures in place to detect, report and investigate a personal data breach.
- GDPR introduces a duty on all organisations to report certain types of data breach to the ICO and in some cases to individuals.
- You have to notify ICO if it is likely to result in a risk to the rights and freedoms of individuals.

Data Protection Impact Assessments

- ICO consider impact assessments to be good practice
- GDPR makes DPIA mandatory in certain circumstances where data processing is likely to result in a high risk to individuals
- DPIA must:
- Describe the nature, scope, context and purposes of the processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate risks.

Data Protection Officers

- DPOs help monitor internal compliance, inform and advise on your data protection obligations, and act as a contact point.
- Under the GDPR, you must appoint a DPO if:
- you are a public authority (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

International

- GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.
- These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Compliance with GDPR Revisited

- **We undertake data-mapping to understand our data sources and storage for all stages of data custody. We look to identify what we are doing with data, how we are protecting data and how we are ensuring we do not infringe on the rights of the subject of that data. That includes that personal data should be obtained for one or more specified purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.**

- **Understanding our data uses for the specific purposes for which the data is being collected (legitimate interests, records of processing, consent, ensuring that data is adequate, relevant and not excessive in relation to the purpose).**

Compliance with GDPR Revisited

- **Protecting the individual – the right to be informed; the right of access; the right of rectification; the right of erasure; the right to restrict processing; the right to data portability; the right to object and rights in relation to automated decision making and profiling.**
- **Implementing appropriate technical and organisational measures to protect data against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**
- **Implementing appropriate controls to avoid that data is transferred to a country or territory outside the European economic area unless that country or territory ensures that an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.**

Q & A