Advanced Capability Solutions

General Data Protection Regulation (GDPR) Overview

(In association with www.ico.org)

Introduction

The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The new regulation will focus on three key main areas :

Transparency

- ✓ Businesses need to be much clearer about how they use personal data
- ✓ Consent rules will be tightened allowing data access harder
- ✓ Access rights will be boosted and delivery times shortened
- ✓ Breaches must be disclosed
- ✓ Audits will be enhanced to support the above

Compliance

- ✓ 'Privacy by Design' means businesses have to ensure data privacy right from the start
- ✓ 'Privacy Impact Assessments' need to be carried out regularly
- ✓ Accountability – All data use must be recorded
- ✓ Data Portability will mean customers can request copies of all of their data
- ✓ 'Right to be forgotten' – Customers have the right to demand all data deletion

Enforcement

- ✓ Tougher enforcement powers for regulators
- ✓ Financial penalties at 4% of a companies worldwide turnover
- ✓ Compensation rights for distress
- ✓ Litigation rights for Civil Society Organisations
- ✓ Data Processors liable in their own right

Who does the GDPR apply to?

The GDPR applies to 'controllers' **and** 'processors'. The definitions are broadly the same as under the DPA – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

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 significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, 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 the GDPR.

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/home

The right of access?

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Charging for Information

- You must provide a copy of the information free of charge. The removal of the £10 subject access fee is a significant change from the existing rules under the DPA.
- However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.
- You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.
- The fee must be based on the administrative cost of providing the information

Provisioning of Information

- You must verify the identity of the person making the request, using "reasonable means".
- If the request is made electronically, you should provide the information in a commonly used electronic format.
- The GDPR introduces a new best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well.
- The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others. Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to (Recital 63).
- The GDPR does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Timescales

- You will have less time to comply with a subject access request under the GDPR. Information must be provided without delay and at the latest within one month of receipt.
- You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.
- Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can charge a reasonable fee taking into account the administrative costs of providing the information; or refuse to respond.
- Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

The right to be informed?

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓

The right to restrict & erase?

Restrict

- You will be required to restrict the processing of personal data in the following circumstances:
- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim

Erase

- The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:
- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.
- Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger

The right to object?

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

✓ Individuals must have an objection on "grounds relating to his or her particular situation". ✓ You must stop processing the personal data unless: ○ you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or ○ the processing is for the establishment, exercise or defence of legal claims. ✓ You must inform individuals of their right to object "at the point of first communication" and in your privacy notice. ✓ This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	✓ You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse. ✓ You must deal with an objection to processing for direct marketing at any time and free of charge. ✓ You must inform individuals of their right to object "at the point of first communication" and in your privacy notice. ✓ This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information". ✓ Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes. ✓ If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

Automated decision making & profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.
Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

Individuals have the right *not to be subject to a decision* when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

You must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation

The right does not apply if the decision:

- is necessary for entering into or performance of a contract between you and the individual;
- is authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or
- based on explicit consent. (Article 9(2)).
- of the decision

Ten Early steps to start preparing

1) Promote awareness
The regulation comes into effect on 25 May 2018 and compliance is mandatory from this date. Key decision makers within your business, including those responsible for budgets, need to be aware of the regulation and its implications and start planning now.

2) Appoint a Data Protection Officer (DPO)
Although not compulsory for smaller businesses it is still worth considering appointing a DPO. It may also be worthwhile establishing a GDPR committee.

3) Carry out an audit
All businesses need to ascertain what personal data they currently hold, where such information has originated from, and with whom it is shared. An audit will also help identify where existing practices fall short of requirements under the GDPR.

4) Train staff early
All staff should be properly trained in order to minimise the likelihood of any breach.

5) Keep records
Businesses need to keep written records in order to evidence how they are compliant with the accountability principle, a central concept of the GDPR.

Ten Early steps to start preparing (cont).

6) Update Privacy Notices
The Data Protection Act 1998 requires businesses to provide certain information to individuals including the identity of the business and intended use of the information. This is often given in the form of a Privacy Notice. The GDPR extends the required information to be given to an employee, for example the retention periods of personal data. Privacy Notices should be reviewed and updated.

7) Be clear on Consent
It must be as easy for an individual to withdraw their consent as it was to provide it in the first place. Businesses will need to carefully review their existing procedures and forms in relation to consent to ensure they are compliant with the GDPR.

8) Review data protection policies
Employers will need to review and likely update their existing contracts of employment, Terms & Conditions and data protection policies to ensure they are compliant with the GDPR.

9) Data Protection Impact Assessments (DPIA)
DPIAs will be mandatory when planning a new initiative, particularly if that involves new technologies and if it involves "high risk" data processing activities. Monitoring individuals or processing special categories of personal data are likely to be high risk.

10) Regularly check for updates
Some details of the GDPR are still being finalised. The ICO publish monthly updates on their website www.ico.org.uk and we would therefore advise you to check this on a regular basis for up to date guidance.

How to Contact Us

London Head Office
60 Cannon Street
London
EC4N 6NP

+44 (0) 207 078 1906

India Delivery Centre
425, 4th Floor, Tower B-3
Spaze I-Tech Park
Sohna Road, Sector 49
Gurgaon, India – 122018
India

info@acsconsulting.com

@ACSConsultingUK

www.linkedin.com/company/advanced-capability-solution

www.acsconsulting.com


Outcomes that Inspire.