Ready, set … GDPR!

HILLYERMcKEOWN

Helping you to prepare for 25th May 2018

The General Data Protection Regulations (GDPR) is a major change which will largely replace the Data Protection Act on 25th May 2018. The GDPR will offer new rights for the privacy of individuals, and businesses must comply by May 2018. Key changes include:

- An increase the responsibility of people and businesses which use and store peoples' data, including any contact information.
- Businesses can be fined 2-4% of their global turnover or between €10 – 20M, whichever is greater.
- Businesses will be required to report a data breach to the ICO (Information Commissioner's Office) within 72 hours.

Countdown to GDPR

If you are currently subject to the DPA, you are likely to be affected by the GDPR

10. Raise awareness of GDPR

Discuss at board level and throughout the business the potential impact of GDPR.

9. Roles and responsibilities

Determine who is accountable for the day to day control of collecting, storing and processing any personal data.

8. Appoint a data protection officer (DPO) and supporting team

Appoint a DPO (the ICO has clear guidelines on who needs to appoint a DPO) and representatives from departments responsible for personal data to coordinate the organisational changes needed to comply with the new law by May 2018.

7. Data Protection Impact Assessment (DPIA) for personal data

Perform a risk assessment for each department, including the lawful basis for handling someone's data.

6. Review consent

How do you seek, record and manage consent for collecting, storing and processing types of personal data?

5. Audit trail

Review the processes and systems in place to ensure security, accountability and transparency.

4. Review legal documentation

Update individuals' rights and privacy information such as privacy notices to make compliant with the new law.

3. Subject access requests

Define how your business plans to handle requests from people to access their data according to the new GDPR.

2. Update policies and procedures with third parties

Is the data you hold shared outside your organisation (who, how, where?), update how you manage the flow of personal data.

1. Final testing and review ready for GDPR 25th May 2018

- Complete final staff training on updates to new policies, processes and procedures for each aspect of personal data management.
- Review and test personal data handling across the business, within departments and for the main individuals who have responsibility for handling personal data.
- Plan for ongoing GDPR compliance by putting in place comprehensive auditing and reporting to ensure the continuation of accurate, compliant, and transparent data management.

"Biggest change to data protection laws in a generation."

Elizabeth Denham, *Information Commissioner's Office (ICO)*

Further guidance from the ICO: https://ico.org.uk/for-organisations/data-protection-reform/

Contact our legal team: enquiries@law.uk.com and *see Guidance Notes overleaf*

GDPR Guidance Notes & Glossary of Terms

Guidance notes

The new rules will strengthen the rights of individuals to say how their personal data is collected, stored and used by people and organisations. The new law will clearly define how data is handled across borders, respond to the digital economy and reflect today's ways of doing business. The GDPR applies to data controllers and processors, the definitions of which are broadly the same as under the current Data Protection Act (DPA).

GDPR affects organisations within the EU, or organisations outside of the EU which offer goods and services to individuals within the EU. Leaving the EU will not affect the timeline for the change in the law.

Please visit the ICO website for exclusions to particular rules
https://ico.org.uk/for-organisations/data-protection-reform/

Glossary

Access to electronic records
User accounts must have individuals who are authorised and can remove information when it is no longer appropriate.

Consent
Individuals must actively provide consent (or opt-in) to receiving marketing materials according to the DPA and Privacy and Electronic Communications Regulations (PECR). Businesses which buy in lists must have sought assurances about the accuracy and origins of the lists. Businesses must identify themselves in marketing and permission to make contact must be initial and ongoing.

Data breach
Under the GDPR, it will be necessary to report a breach to the ICO within 72 hours where there is a high risk to an individual's rights and freedoms. Your business must have in place a mechanism to notify both the individual and the ICO following a data breach.

Data disposal
Organisations need to have a plan covering which details and for how long manual and digital records are to be kept. Records are to be destroyed appropriately according to the GDPR.

Data sharing
Your business will be required to keep an up to date and accurate record of all decisions to share personal data. Training must be provided to ensure members of staff have the information required to be able to make decisions about sharing personal data with third parties. Regular compliance monitoring will be necessary.

"Get it right to see the business benefit."
Elizabeth Denham, *Information Commissioner's Office (ICO)*

Managing data records
This includes applying minimum standards for creating paper and digital records. Paper records must be tracked when storing or moving offsite or between offices. Under the GDPR there must be a legitimate purpose for using personal data before it is collected and data is to be relevant for the purpose. A process must be in place for periodically checking and updating records (such as when people unsubscribe and do not wish to receive further information). An inventory is to be kept centrally for manual and electronic record keeping. Protect personal data for new projects, for data processed by others on behalf of the organisation or personal data transferred outside the European Economic Area (EEA).

Personal data
Personal data is any type of information belonging to an individual which can be identified directly or indirectly to that person. This includes contact information such as IP addresses, HR data, and lists used for marketing. The GDPR will cover paper and digital information, and manual and automated processes (which may require the data to be modified so that it cannot be attributed to the original person). There must be a lawful basis for processing personal data as explained in a privacy notice.

Security
An organisation must ensure senior management has approved the information security policy which complies with relevant laws and regulations. Written agreements must be obtained from third parties, including protecting data accessed by suppliers and providers. Physical and digital working procedures are to comply with GDPR.

Subject access request under GDPR
Your business must be able to handle requests from people to gain access to their personal data within the new timeframe and provide any additional information as requested. The necessary training and resources should be in place to handle subject access requests.