GDPR in 10 Questions

2018

There's only five months to go until the new General Data Protection Regulations (GDPR) come into force on 25 May 2018. All UK businesses will be required to comply or run the risk of crippling fines.

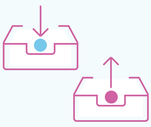
Here's what you need to know:

1 As a decision maker are you aware the law is changing with GDPR?

- Individual rights strengthened
- New responsibilities such as Transparency, Consent requirements, Privacy by design, Data Protection Officer (DPO), Data breach notification have been introduced
- Penalties for breach of rules up to 4% turnover
- **ALL** staff need knowledge on GDPR

2 Can your company and employees apply the principles of personal data?

- Lawfulness, fairness and transparency
- Purpose of data limited - specified, explicit and legitimate purpose
- Storage limitation for no longer than is necessary
- Data minimisation (adequate, relevant and limited to those which are necessary)
- Accuracy and up to date; inaccurate personal data are erased or rectified without delay
- Integrity and confidentiality



3 Does your company have the correct procedures to ensure you deliver the rights of individuals under GDPR?

- The right to know the information you hold on them
- The right to have access to their personal data
- The right to rectification of the information you hold on them
- The right to be forgotten (erasure of the information you hold on them)
- The right to restrict the use of the information you hold on them
- The right to data portability of the information you hold on them
- The right to object to the information you hold on them
- The right not to be subject to automated decisions and profiling

4 Is your company holding sensitive data in your systems

- Racial or ethnic origin
- Political opinions or trade union membership
- Religious or philosophical beliefs
- Data concerning health or genetic data (new)

5 Does your company have processes to provide all data you hold on a client if requested?

- You will **not** be able to charge for such a request
- You need to comply within **1 month**
- You can refuse or charge for requests but you must tell the individual they have the right to complain to the supervisory authority and to a judicial remedy

6 Can your company demonstrate you have the necessary basis to hold the client data in your systems?

- Consent is **active**, and does not rely on silence, inactivity or pre-ticked boxes
- Needs to be obtained using distinguishable and clear language not "bundled" with other written agreements or declarations
- Right to withdraw clearly proposed to the data subject

7 Do you have the right procedures in place to detect, report and investigate a personal data?

You **must** notify:

a) Supervisory authorities without undue delay and within **72 hours** of discovery

b) Clients without undue delay if the leaked data poses a "high risk to their rights and freedoms", for example, if the breach might leave them open to financial loss

8 Privacy by design

- Implement appropriate technical and organisational measures to carry out data protection principles in an effective manner and to integrate the necessary safeguards

9 Have you designated a data protection lead in your organisation?

- Required if you undertake work for a public authority, carry out large scale systematic monitoring of individuals or hold data relating to criminal convictions and offences

Duties include:

- Informing and advising the organisation about their GDPR obligations
- Monitoring compliance with the GDPR
- To be the first point of contact for supervisory authorities and for individuals

10 Outsourcing activities - is your supplier agreement aligned to GDPR?

- Select and sign trustful and reliable partners providing sufficient guarantees and scope the partners' responsibilities and activities
- Does the partner have a data protection lead
- Insist on appointment of a local representative when outsourcer is located outside the EU
- Prevent partner from engaging another outsource partner without authorisation

www.keytime.co.uk | email support@keytime.co.uk | 0161 484 3500

Keytime