General Data Protection Regulation

TRAINING & AWARENESS

created by K7 COMPLIANCE LTD

GDPR FACTS & PURPOSE

- Enforced on the 26th May 2018
- The most significant data security law in the world
- Protecting the rights, privacy and freedoms of EU & UK residents
- Removing barriers to business facilitating the free movement of data throughout the EU
- Relates to the processing of personal data within the EU & UK

KEY DEFINITIONS

- **Processing** - any operations which is performed on personal data, such as collection, recording, organasation, storage , adaptation or alteration.
- **Controller** - the person or other body who determines the purposes and means of the processing of personal data.
- **Personal Data** - any unformation relating to a natural person (data subject)
- **Data Subject -** a living, identifiable natural person, who can be identified directly or indirectly by an identifier

KEY DEFINITIONS (continued)

- **Subject Access Request (SAR)** -a request from a data subject for personal information to an organisation
- **Data Breach** - a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of all access to personal data
- **Data Protection Impact Assessment** - a risk assessment examining the likelihood of a data breach occurring

GDPR PRINCIPLES

1. Lawful, transparent and fair
2. Purpose limitation
3. Minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

GDPR PRINCIPLES

Lawfulness Principle

1. Consent of the data subject
2. Processing is required for the performance oa contract with the data subject
3. Processing is required for compliance with a legal obligation
4. processing is required to safeguard the vital interests of a data subject
5. processing is required for a task carried out in the public interest
6. Processing is necessary for the purposes of legitimate interest , pursued by the controller where such interests are outweighed by the interests rights or freedoms of the data subject

GDPR PRINCIPLES

Consent

- An indication of the data subjects wishes which affirmatively and clearly indicate consensual acceptance by the data subject of the processing of their personal data
- consent means freely given, specific and informed. In some cases a special form of consents called explicit consent will be needed

GDPR PRINCIPLES

Transparency

- information about processing must be disclosed clearly and thoroughly
- it must be provided in an accessible format and obtainable manner
- the provided information must be free, as long as the requests are from somebody identifiable on the number of requests doesn't exceed a predetermined amount

GDPR PRINCIPLES

Fairness

- data subjects have rights which allow them to be treated fairly
- where a response is required, the controller or processor have one month to reply

GDPR PRINCIPLES

Purpose limitation principle

- Personal data should be collected for specified, legitimate and explicit purposes and must not be further processed in a way which is incompatible with such purposes

GDPR PRINCIPLES

Minimisation principle

- Personal data must be relevant, added quotes unlimited to what is necessary in relation to the purposes for which that data is processed
- In other words - only what we need, nothing more

GDPR PRINCIPLES

Accuracy principle

- Personal data must always be up to date and actions should be taken to avoid storing old or redundant data
- action must be taken to ensure that inaccurate personal data with regard to the purposes for which they are processed, should be raised or rectified without delay

GDPR PRINCIPLES

Storage limitation principle

- kept in a form that permits identification of data subjects for no longer than is necessary , for the purposes for which the personal data is processed
- personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest , scientific or historical research purposes, or statistical purposes , subject to implementation of the appropriate technical and organizational measures required by this regulation , in order to safeguard the rights and freedoms of the data subject

GDPR PRINCIPLES

Integrity and confidentiality principle

- Personal information should be processed in a manner of ensures appropriate security of the personal data
- taking into account state of the art , cost of implementation on the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects

GDPR PRINCIPLES

Accountability principle

- both the data controller and data processor have responsibility for, i must be able to prove compliance with all gdpr principles
- the gdpr requires businesses to show how they comply with the principles, through demonstrating they have a robust process is in place to handle personal information and have affected documentation documenting the decision‘s they take about a processing activity
- the ICO can audit businesses to check compliance with the accountability principle

THE RIGHTS OF THE DATA SUBJECT

- **the right to be informed** - data subjects should be clear about what why and in what way personal information will be processed . This is usually provided by a privacy policy
- **the right of access** - data subjects have the right to learn what personal information is held on them by whom and why. This is triggered by a subject access request
- **the right to rectification** - Data subjects can request rectification of that personal data if it is wrong or inaccurate

THE RIGHTS OF THE DATA SUBJECT

- **the right to erasure** – data subjects can request to be forgotten through having the personal information erased
- **the right to restrict processing** - data subjects can ask organisations to stop processing that personal data
- **the right to data potability** - data subjects can ask for the personal data in machine readable formats also have it sent to another organisation

THE RIGHTS OF THE DATA SUBJECT

- **the right to object** – data subjects can object to their data being processed by an organization
- **automated decision making and profiling** – protection against automated systems that could have a significant impact on peoples lives - loan applications, jobs applications

DEMONSTRATING COMPLIANCE

- training and awareness of everypne
- effective policies and procedures for data protection
- Establishing key data protection objectives
- effective management and reporting of subject access requests and data breaches
- data encryption procedures and other information security best practice
- internal audits and information security tests

IMPACT OF COMPLIANCE FAILURE

- If a data subjects rights are breach they can Sue you in your country , all theirs , for material and non material damage. There is no upper limit set by the gdpr . They can Sue you individually or collectively
- administrative fines from the ICO up to 20,000,000 euro or 4% of annual global turnover, whichever is the greatest

DATA BREACHES

- personal data breach refers to an event that results in the Los, desctruction, alteration, unauthorised disclosure of , or access to, personal data
- obligations for the data processor to notify the data controller time for the data controller to notify the ICO (if applicable) and the data subjects
- it is up to the organization whether or not to report a breach to the ICO
- the data breach must be reported within 72 hours of the breach occurring

SUBJECT ACCESS REQUESTS

- a request triggered by a data subject to an organisation to gain confirmation that the organisation is processing their personal data or to discover what personal data is held by them or to learn what personal data is disclosed to other organisations
- subject access requests should be responded to within a month
- Subject access request can be written, verbal , electronic or physical

DATA PROTECTION OFFICER

- advises organisations of the data protection obligations
- monitors compliance with the gdpr including assigning responsibilities , awareness raising I'm training of stuff involved in the processing of data
- provides advice when requested with regard to the data protection impact assessments and monitors its performance
- to act as the contact person for the ICO and to co-operate with them on issues related to the processing of personal data

FURTHER READING

- www.ico.org.uk
- www.gdpr-info.eu
- www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

TAKE THE TEST

Please click on the link below to take a short test to measure your understanding of the GDPR. There are no pass or fail marks and the test should take you no longer than 15 minutes,

Take the Test