Icon Training - Data Protection Training and Awareness

What is the GDPR?

The EU General Data Protection Regulation, or GDPR, is a significant enhancement to the old Data Privacy Directive. This law aims to protect the personal data of individuals while that data is being used by various organisations. As it is a Regulation, and not a Directive, it is now law which is enforceable by the various EU legal entities.

What is Personal Data?

Personal data is information relating to an individual, including, but not necessarily limited to name, contact details, identity number, bank details, race, gender, age, health status, email address, location, online identifier and the like

What are Special Categories of Personal Data?

This is sensitive information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

What is a Data Subject?

A data subject is the identifiable, natural person to whom personal data belongs. For example, some of the data subjects of an organisation could be its customers and employees

What are the Rights of data subjects?

In order to protect the rights that the GDPR grants to data subjects, organisations need to observe the following:

- The head of any organisation is accountable for complying with the Regulation
- Personal data must be collected and used only for the specific and lawful purpose for which the organisation is established
- Only the essential amount of personal data must be collected from the data subject
- The personal data of a Child may only be collected and used upon consent of a parent or guardian
- Personal data must, as far as is practicable, be collected directly from a data subject
- Do not retain personal data for longer than is necessary for that specific purpose
- Where the personal data might be used for a purpose different to the original reason for collection, in most cases, the data subject's consent must be confirmed
- Organisations must ensure that the personal data remains complete, accurate and up to date
- Always be transparent in your communications with data subjects
- Protect personal data from loss, theft and unauthorised access
- Where personal data are processed by an external service provider (called a processor), ensure that Contracts are in place which demand that the processor also complies with these conditions
- Where personal data must be shared with or disclosed to other Controllers it is good practice to have in place a data sharing agreement

- Have a system in place to notify data subjects and the Supervisory Authority of any breaches in security
- Have a system in place to allow data subjects to access and manage their personal data
- You can only market electronically to data subjects if they are your bona fide customers
- You cannot email a prospective client asking for consent to market electronically to them
- All electronic marketing to your clients must contain a mechanism for them to object to such marketing
- Your data subjects have the right not to be subject to any decisions which are based solely on automated processing, which includes profiling, and which produces legal effects for them or significantly affects them
- Ensure that whenever consent is needed and given, you retain the evidence of consent having been given
- Consent should be given by a clear affirmative act establishing a **freely given, specific, informed and unambiguous indication** of the data subject's agreement

What is a Controller?

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Our organisation is a controller.

What is a Processor?

The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. For example, if our organisation were to outsource the processing of our payroll to an external organisation, that organisation would be the processor. Of course, if our organisation is to process payrolls on behalf of other controllers, we would also be a processor - and, therefore, both controller and processor

What is a Data Protection Policy?

A Policy is internal to an organisation and demonstrates management's intent with regards to compliance with legislation such as the GDPR

What is a Privacy Notice?

A Privacy Notice draws special attention to the manner in which our organisation is complying with the GDPR. It is usually displayed at points where we collect personal data and informs data subjects as to their rights

Data Subject's access to his or her Personal Data

Data subjects have the right to enquire whether an organisation holds their personal data and also to request the records or descriptions of those records. They have the right to challenge and even stop the processing of their personal data. They may request that their personal data be changed - e.g. where a name, surname or contact details change. When a data subject makes a request for access, the data subject's identity must be confirmed before you may continue with the response. Our data protection management system, has a special section to assist with data subject access requests. If you recognise a request for information you need to alert your manager.

What is 'limited personal use'?

Often the line between personal use and organisation use of systems becomes blurred. Our systems are primarily and exclusively for organisation use. Where we allow limited personal use of our organisation's IT systems you must be aware of the following:

- DO NOT make personal use, of an unreasonable amount, of our organisation's network or other technology resources (e.g. to stream audio or video, download or store large files, or large amounts of printing)
- DO NOT allow personal use to interfere with your productivity or the productivity of others who are doing organisation work
- DO NOT violate copyright, data protection laws, or licensing arrangements (e.g. file sharing of content protected by copyright, such as movies and music)
- DO NOT use our organisation's IT systems and services to run or support a private organisation
- DO NOT use our organisation's IT systems and services to distribute SPAM, personal solicitations or unsolicited advertising
- DO NOT assume that our organisation has an obligation to store or recover your personal content saved on organisation IT systems, if lost
- DO NOT break local laws, cause harm or offense to others or negatively impact the organisation's reputation or interests

How do I play my part in protecting Personal Data?

Understand and respect the rights of data subjects

Be aware that some information within our organisation is classified as 'Confidential' and must be treated accordingly

All personal data in our organisation is classified as 'Confidential'

Understand what we mean by the 'Acceptable Use' of our digital systems

Use strong passwords and keep them to yourself

Understand how to recognise suspicious emails and links

Think twice before clicking on any suspicious links

Keep your workstation clear, especially with regards to sensitive information

Practice discretion when you are outside and discussing our organisation

Keep our IT equipment safe, especially when you are outside the organisation premises

Be aware of the limitations we set with regards internet access and usage

Understand what we mean by 'limited use' of our organisation's systems for personal reasons

If you know your rights as a data subject, it will be much easier for you to apply this knowledge in the execution of your own job