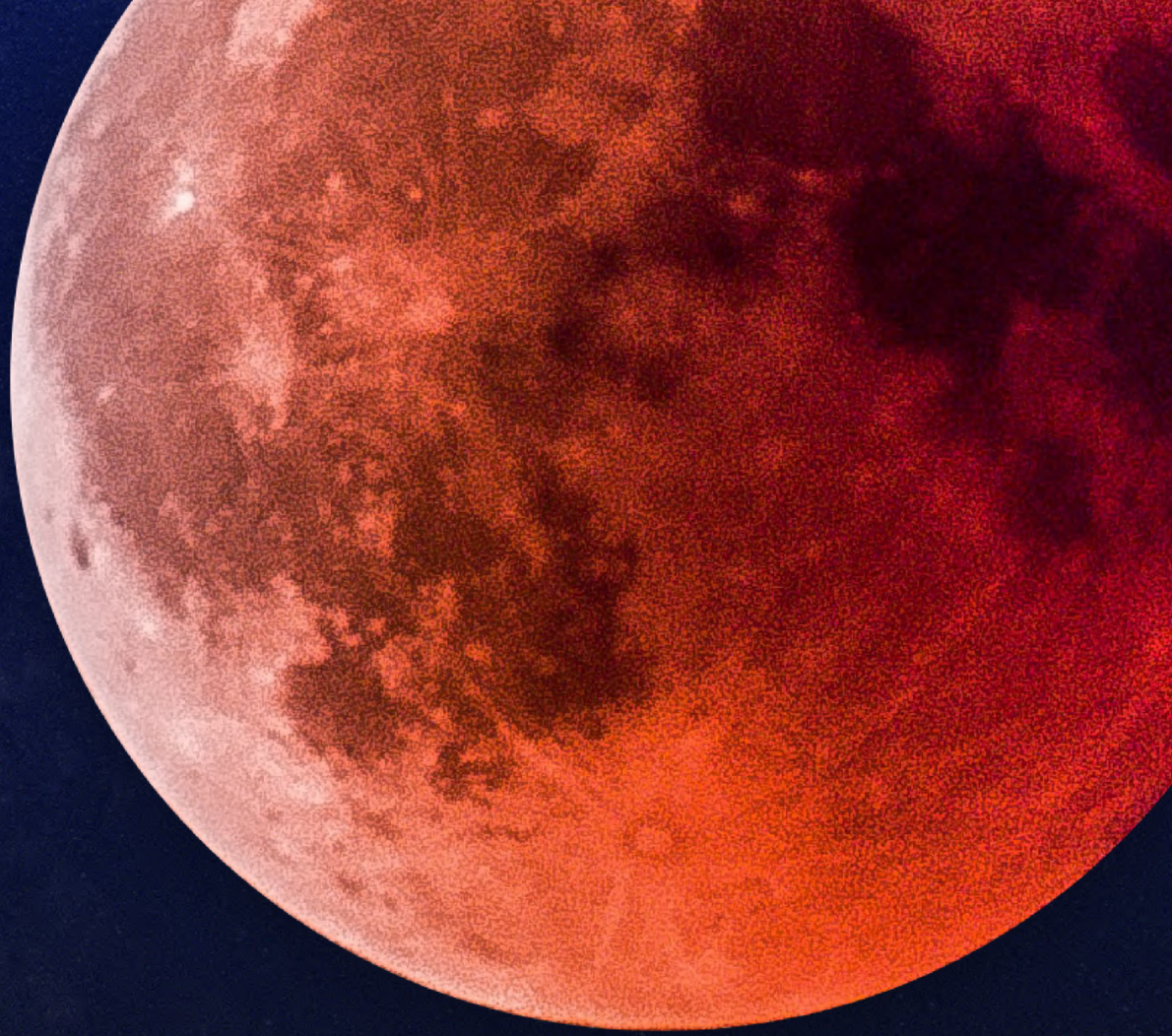
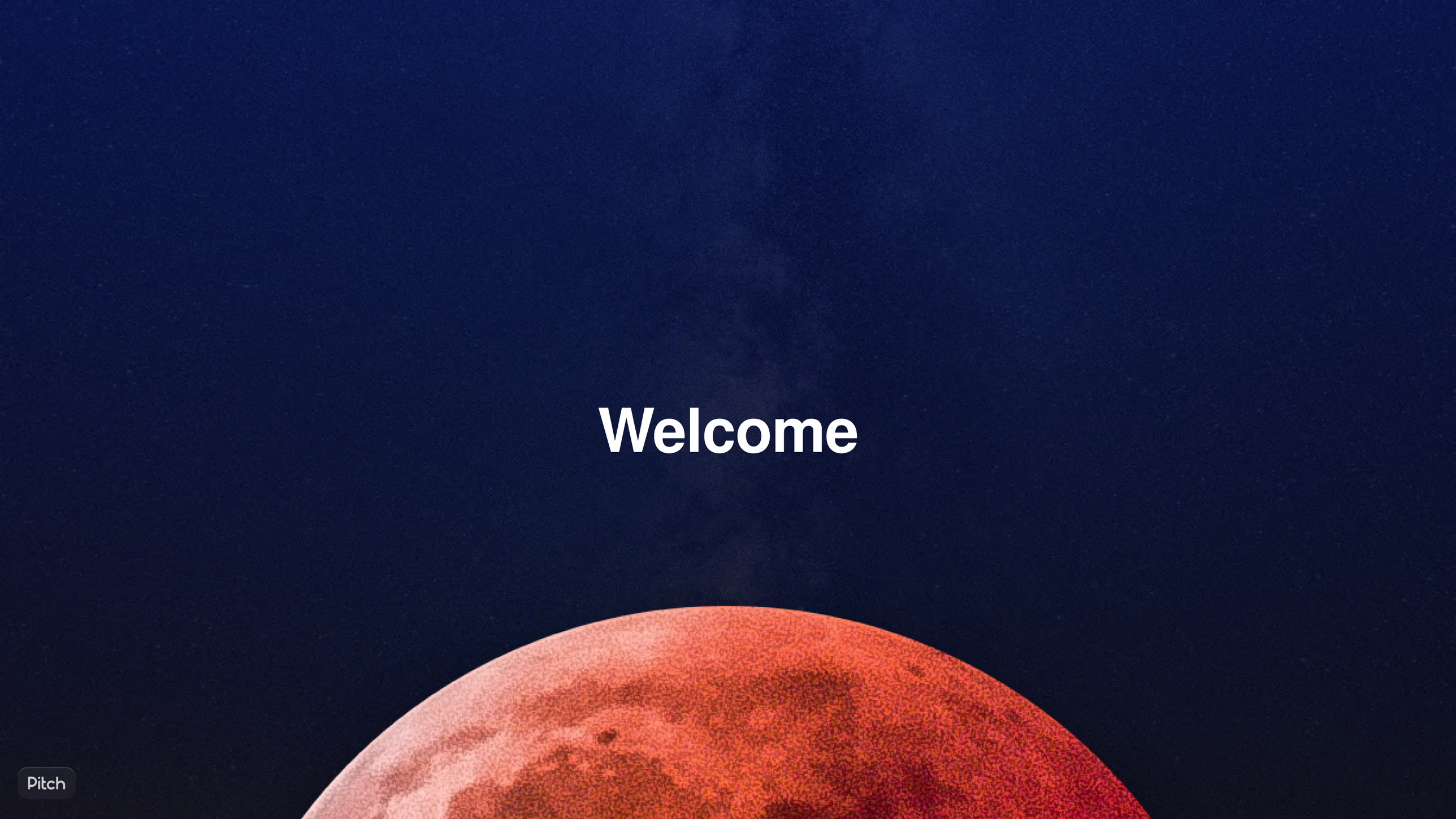


GDPR

Data Protection and Privacy Training

Welcome



What is GDPR?

- GDPR stands for General Data Protection Regulation is a legislation designed by the European Parliament back in 2016 when the European Union recognized the importance of data protection for its citizens, especially as we see the changes that technology has made in our lives.
- The EU GDPR sets out in law when, under which conditions, personal data can be collected, what it can be used for, and the rights of the person the data belongs
- GDPR applies to any business that handles EU citizens' data, even if the business is not physically located within the region.

Do All Businesses Need to Comply?

1

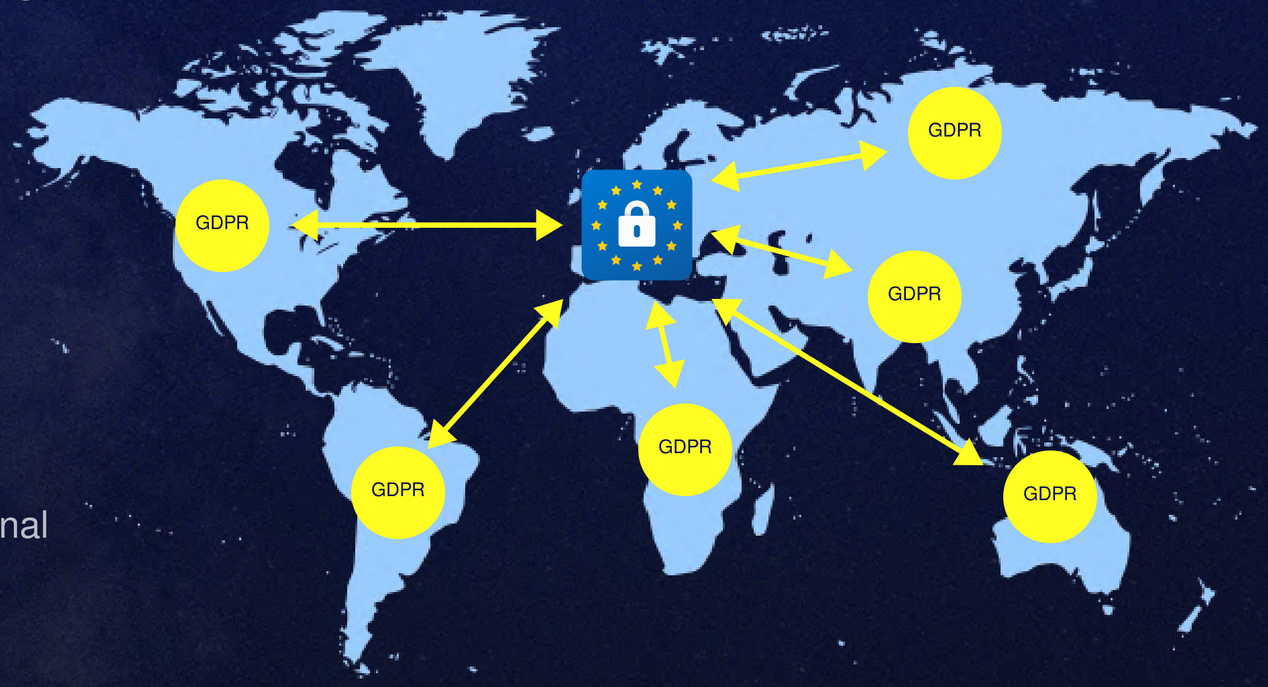
The GDPR applies to both data ‘controllers’ and ‘processors’.

- Data controllers determine the purpose and manner in which data is processed.
- Data processors are any third-party undertaking data processing on behalf of a controller.

2

Companies that must comply include those that are:

- Based or have a presence in an EU nation
- Do not have a presence in the EU, but deals with personal data of EU citizens, in the course of offering goods and services either for free or for payment



Principles for Processing Personal Data

LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data shall be processed when it is necessary and meets one of the lawful basis for processing.

PURPOSE LIMITATION

Personal data shall be collected for **specific, explicit, legitimate** and **limited** purposes. We should not process this information for any other purpose other than its original intent unless it is permitted by law.

INTEGRITY AND CONFIDENTIALITY

Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using technical or organizational measures.

STORAGE LIMITATION

Personal data shall be kept in a form which permits identification of the person for no longer than is necessary for the processing purpose.

DATA MINIMISATION

Personal data shall be adequate, relevant and limited to what is necessary to properly fulfil the processing purposes.

ACCURACY

Personal data shall be accurate and, where required, kept up to date.

ACCOUNTABILITY

The controller shall be responsible for, and be able to demonstrate compliance with the Data Protection Principles

The GDPR provides the following rights for data subjects (individuals)

THE RIGHT TO BE INFORMED

The right to know how personal data is used in clear and transparent language.

THE RIGHT OF ACCESS

The right to know and have access to the personal data held about an individual.

RIGHT TO RECTIFICATION

The right to have data corrected where it is inaccurate or incomplete.

RIGHT TO BE FORGOTTEN

The right to have personal data erased.

RIGHT TO RESTRICT PROCESSING

The right to limit the extent of the processing of personal data according to an individual's wishes.

RIGHT TO DATA PORTABILITY

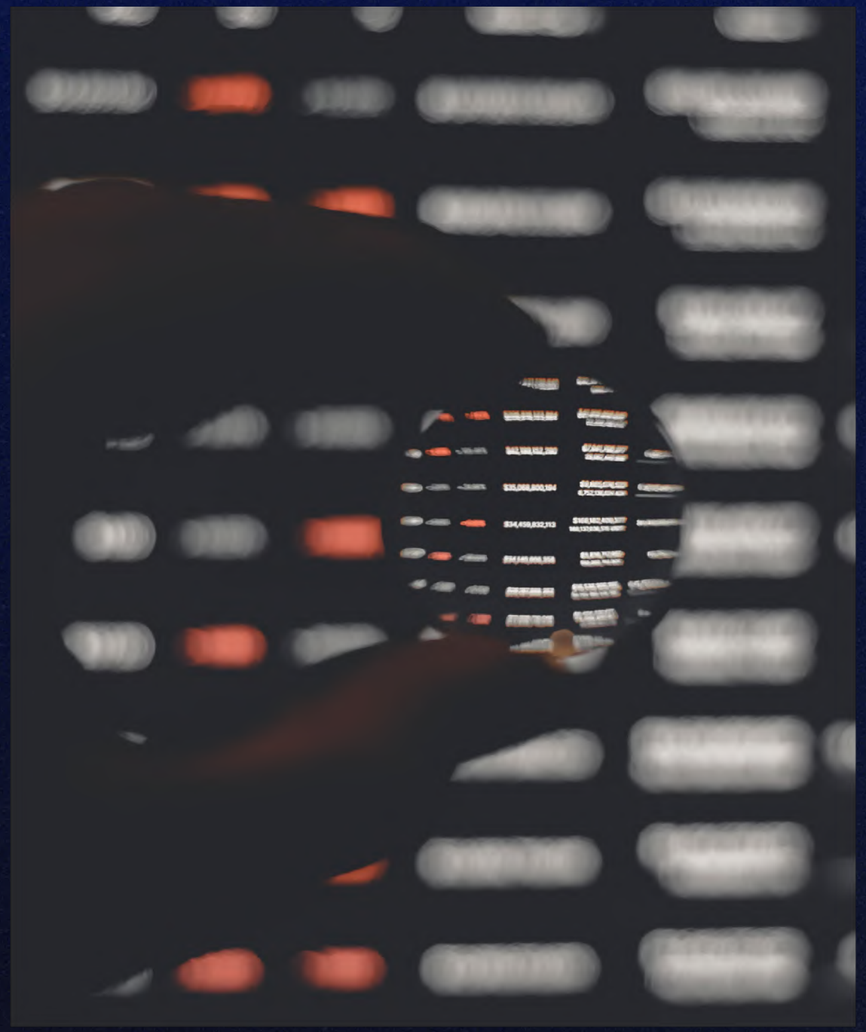
The right to receive and transfer data in a common and machine-readable electronic format.

RIGHTS RELATED TO AUTOMATED DECISION-MAKING AND PROFILING

The right not to be subject to decisions without human involvement.

RIGHT TO OBJECT

The right to complain and to object to processing.



Maintaining a Processing Register

The GDPR Article 30 is extremely specific in its requirements, so even if an organization has previously performed data mapping, it will need to be updated or redone to meet the GDPR requirements.

The following information must be documented

- The name and contact details of your organization
- The purposes of your processing
- A description of the categories of individuals and categories of personal data
- The categories of recipients of personal data
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place
- Retention schedules
- A description of your technical and organizational security measures

My responsibilities as an employee

All employees hold a personal responsibility for ensuring that personal information is used fairly and lawfully. These include:

- Appropriate and secure storage for paper and electronic records
- Encrypt data on laptops, tablets, memory sticks, etc.
- Authorised access only, no password sharing
- Double-check your correspondence addresses and attachments
- Do not share information with third parties without data sharing agreements approved by the Data Protection Officer
- Destroy records appropriately and securely
- Be aware of your cloud usage
- If you are aware of a security incident (or a near miss), report the incident immediately to the designated officer so that the incident can be investigated and managed.

What Constitutes a Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of personal data.

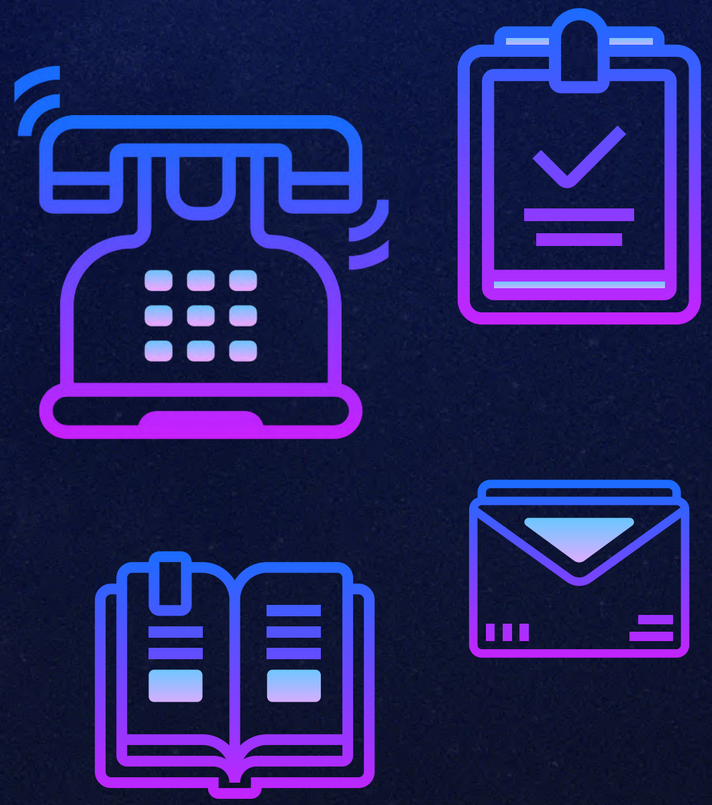
A breach could result from many activities.

- Accessing more than the minimum necessary information
- Failing to log off when leaving a workstation
- Unauthorized access to Personal Data
- Sharing confidential information, including passwords
- Having patient-related conversations in public settings
- Improper disposal of confidential materials in any form
- Copying or removing Personal Data from the appropriate area

Data breach notifications

The below steps need to be followed in the event of a breach.

1. Assess the risk to individuals’ rights and freedoms
2. Notify:
   - Supervisory Authority (Information Commissioner's Office (ICO)) within **72 hours**
   - Data subject (high risk only)
   - Other organisations/regulators (if required)
3. Document your decision making



THANK YOU

Stay Safe