# UK GDPR (General Data Protection Regulation) Factsheet

**The aim of data protection law is to ensure organisations use information about individuals in a fair and regulated manner.**

**If you are an organisation in the UK processing UK personal data, you must follow UKGDPR.**

Why is data protection important?

* It protects the privacy of individuals
* Prevents misuse of their information

Laws

* UK GDPR and Data Protection Act 2018
* Enforced by the ICO ([Information Commissioners Office](https://ico.org.uk/))

Who does UK GDPR apply to?

* All UK-based business or organisations processing data in the UK
* If you are outside of the UK or processing data from outside of the UK, other GDPR may apply; read more: [The UK GDPR | ICO](https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/)
  + E.g. there are rules on transfers of personal data between the UK and the EEA.

Developments in GDPR

* In the UK, the EU GDPR was replaced by the UK GDPR following Brexit in January 2021.
  + The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.
  + The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to:
    - offering goods or services to individuals in the UK; or
    - monitoring the behaviour of individuals taking place in the UK.
* In March 2023, the [Data Protection and Digital Information Bill](https://bills.parliament.uk/bills/3430) was reformed to make further changes to UK GDPR, although the main principles still apply.
  + Legitimate interest: A grey area under GDPR, the Bill expands the scope of legitimate interest so that charities can use it as a lawful basis to recruit new supporters.
    - Charities will be able to contact existing supporters by email, using the so called ‘soft opt-in’ previously only specified for commercial organisations.
    - Individuals still have the right to opt out, but charities can confidently approach new potential supporters who may have a legitimate interest in their charitable work.
  + The Data Protection Officer requirement is being replaced with the ‘Senior Responsible Individual’
    - This must be a member of senior management and will be responsible for monitoring data protection compliance.
  + Multinationals with operations in both the UK and the EU/EEA will have to comply with the GDPR
  + Read all changes to the 2023 bill here: [ICO - View on the Data Protection and Digital Information Bill (DPDI Bill)](https://ico.org.uk/about-the-ico/information-commissioner-s-response-to-the-data-protection-and-digital-information-bill/information-commissioner-s-view-on-the-dpdi-bill/)

Categories of Protected Data

* **Personal data:** Any data which directly or indirectly identifies a person, e.g., name, email, telephone
* **Sensitive/special category data:** Data which requires extra protection,   
  e.g., health records, racial origin, religious beliefs, political views, sexual orientation
  + It is prohibited to collect this unless specific legal condition or exemption
  + Explicit consent must be given by individual

# What is data processing?

Processing includes storing, collecting, using, disclosing, recording or erasing data.

Data Processing Terms  
There are three roles in data processing as below. Read more here; [What are ‘controllers’ and ‘processors’? | ICO](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/#:~:text=a%20processor%20as%3A-,%27processor%27%20means%20a%20natural%20or%20legal%20person%2C%20public%20authority,interests%20rather%20than%20their%20own.)

# Data Protection Principles

There are seven data protection principles which you must follow:

1. Lawfulness, fairness and transparency  
   Be open and honest about what you plan to do with data and only process in standard ways (e.g., online forms, databases).
2. Purpose limitation   
   Only collect data for specific, explicit and legitimate purposes. Do not use data collected for one purpose for another activity.
3. Data minimisation  
   Only collect what you need! Ask yourself why you need each piece of data.
4. Accuracy  
   Keep everything up to date and take steps to ensure data is accurate (e.g., have set fields to check that email addresses are in the right format).
5. Storage limitation  
   Do not keep data for longer than necessary, have a data retention policy.
6. Integrity and Confidentiality (security)  
   Process data in secure way to prevent data breach/unauthorised use. Use technical and organizational security procedures (e.g., password protection, restricted access).
7. Accountability  
   Demonstrate compliance with policies and that you have taken steps to keep data secure.

# UK GDPR

UK GDPR has accountability principles as follows:

* Demonstrate compliance
  + Consider data protection at start of any new project
  + Undertake data protection impact assessments for high-risk projects
  + Maintain internal records
  + Ensure DP principles are automatically incorporated into processes
  + Appoint a “Senior Responsible Individual” who is in charge of data protection
  + Have policies & procedure in place and provide staff training
* Consent:
  + People must opt-in to consent (i.e., tick a box to agree, not untick to refuse)
  + Right to withdraw consent at any time
  + Separate consent requirement for each different use of data
  + Keep records to demonstrate consent
* Privacy Notices:
  + Be clear about how you will use the data, who it will be shared with and how long you store it for – this is known as a Privacy Notice
* Individual’s Rights
  + **Right to restriction** – right to block use of their data, e.g. if someone complains that data about them is inaccurate
  + **Right of access** – right to ask for copy of their data, Subject Access Request (SAR)
  + **Right to object** – to use of their data (although business can still use if compelling grounds)
  + **Right to erasure** – “the right to be forgotten” request to delete data
  + **Right to data portability** – individuals are entitled to receive an electronic copy of their data, and sometimes have it transferred to other business
  + **Right to rectification** – request to correct any incorrect data
* Notification of data breaches:
  + To ICO: Mandatory notification of breaches that could result in significant detrimental effect (within 72 hours)
  + To individual: Mandatory if high risk to individual (financial risk, loss of confidentiality and discrimination)
* Fines for data protection breaches
  + Lower level – up to £8.7 mill or 2% of annual turnover (whichever is higher)
  + Higher level – up to £17.5 mill or 4% of annual turnover (whichever is higher)

How you can help your employer

* UK GDPR defines data breach as “a breach of security leading to unlawful deletion, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.
* Personal data breaches include:
  + **Destroyed data** – through unforeseen circumstances e.g. fire or software-failure
  + **Unauthorised access** – someone accesses data who is not authorised to do so
  + **Accidental loss** – through mishandling of data, not having proper security in place
  + **Human error** – e.g. sending personal information to the wrong person
  + **Corrupt data** – where data is corrupt (e.g. through viruses)
  + **Deception –** where data is acquired through deception (e.g. phishing emails)
  + **Cyber-attack** – malware and ransomware attacks, etc.
  + **Password** – inadequate security controls (e.g. weak passwords)
  + **Stolen data** – data or equipment theft, electronically or physically
* How to keep data safe
  + Keep passwords secret
  + Don’t leave IT equipment around without being properly secured
  + Lock computer when away from desk
  + Don’t store data on personal devices or USBs
  + Store papers with personal information securely, e.g., a locked drawer or scan in and password-protect file
  + Don’t send personal data from your work email to your personal e-mail
  + Dispose of data you no longer need to keep
  + Follow IT procedures set by your organisation
* What to do if there is a data breach
  + **Don’t delay** – tell the Senior Responsible Person immediately, no matter how small the breach
  + **Remember your organisation only has 72 hours to notify the ICO of a data breach**
    - Use[Self-assessment for data breaches | ICO](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/) this [determine](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/) if you need to report to the ICO
    - Report a breach here: [UK GDPR data breach reporting (DPA 2018) | ICO](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/)
  + Notification to individuals is mandatory if a breach is likely to result in a high risk to the rights and freedoms of individuals. In these cases you must inform those concerned directly without undue delay.