THE 7 DATA PROTECTION PRINCIPLES

THE 7 DATA PROTECTION PRINCIPLES are a key part of the General Data Protection Regulation (GDPR). The GDPR comes into force in the UK on the 25th May 2018. Along with the new Data Protection Bill, the GDPR is the biggest shake up of data protection law in the UK since 1998.

What are the 7 data protection principles?

The 7 data principles are:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data Minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

Why do the principles matter?

The data principles outline what an organisation or business must do to protect your data security, protect your identity and ensure your privacy is not put at risk when they process your personal data.

What does processing mean?

Processing is what happens to your personal data when you hand it over to an organisation.
The term "processing" covers the following actions all of which can be done to your personal data:

- Collection
- Recording
- Organisation
- Structuring
- Storage
- Adaptation and alteration
- Retrieval
- Consultation
- Use
- Disclosure
- Dissemination
- Making available
- Alignment or combination
- Restriction
- Erasure
- Destruction

Principle 1 : Lawfulness, fairness and transparency

Your personal data must be processed lawfully, fairly and in a transparent manner.
An organisation is only lawfully processing data if they have explicitly asked for and received your consent to process your personal data.
Transparency means an organisation must ensure they tell you in clear and easily understandable language why your data is going to be collected, how it will be used and how it will be processed.
It is likely you will find detail of how a processor will handle your data in their terms and conditions or in the privacy policy.

Principle 2: Purpose limitation

Purpose limitation means your data must only be:

- collected for a specific, explicit and legitimate purpose.
- used for the reason you first agreed to.

If your personal data is to be used for another reason the organisation must tell you the new purpose and, if need be, ask for your consent to continue processing the data.
Your personal data can be archived in the public interest, or used, held and shared for statistical, scientific or historical research purposes without your consent.

THE 7 DATA PROTECTION PRINCIPLES

Principle 3: Data Minimisation

Data minimisation means an organisation can only ask for personal data which is adequate, relevant and limited to the purpose of the processing.

For example if you are buying something online, the organisation can only ask for the data they need to process payment and delivery. They cannot ask for further information which does not relate to the purchase.

Asking people for extra information usually benefits the organisation not the individual.

Principle 4: Accuracy

Organisations must ensure that the personal data they hold is accurate, and where necessary, is up to date.

If data held is found to be inaccurate, the organisation must make every effort to quickly correct or erase the errors.

Principle 5: Storage limitation

Personal data which identifies you must only be kept for as long as it serves the purpose for which you originally gave it.

For example, if you have given personally identifiable data to a company in order to make a purchase, the company can only hold the data for the time it takes to process the purchase.

If an organisation wants to hold your data to make purchases easier they must ask for your consent and give you the option to delete your data if you choose.

Personal data can only be held for longer without your expressed consent if it is in the public interest or for statistical, scientific or historical research.

Principle 6: Integrity and confidentiality

Organisations must take security measures to protect your personal data against:

- unauthorised or unlawful processing of personal data
- accidental loss, destruction or damage.

Appropriate technical or organisational measures must be used to ensure your personal data is safe and secure.

Principle 7: Accountability

Accountability is a brand new data protection principle.

It means data controllers must clearly show they are complying with the law and are responsible for the personal data they are processing.

This principle stops organisations pretending to just follow data protection, they must now show they are complying properly.

Don't Forget

- The principles are based on the 6 data principles of the Data Protection Act 1998.
- The new principle is accountability.
- The principles detail the way an organisation must process your personal data.