The Data Protection Act Key Principles:

Fair, lawful, and transparent processing

GDPR states that personal data must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject'. This means that all data controllers must only process data for the purpose they acquired it and with consideration of the data subject's rights. You must have a legitimate reason for processing their data and **never** hold onto it for other purposes.

Furthermore, you must tell the person exactly **what you'll use their data for** and receive explicit consent. When you are acquiring their data, you must offer a clear statement about how you plan to use it before they agree. Keep in mind that you can only provide **opt in** options, not opt out. You must also include information in your privacy policy about why you may need people's personal data.

Purpose limitation

The principle of purpose limitation states that data must only be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'. The only exception to this is purposes relating to public interest and scientific or historical research. However, the controller must have authorisation to do so.

Purpose limitation supports the previous principle: you cannot use data for any purpose other than the one you collected it for. For example, let's say you are acquiring data to complete a transaction with a customer. Without explicit consent, you cannot use that same data for marketing purposes.

It's also important to know that most businesses must notify the **Information Commissioner's Office (ICO)** of how and why they plan to acquire data. Some organisations are exempt, such as if you only process personal data for payroll or for maintaining a public register. If you are unsure about whether you need to notify the ICO, you should contact them directly and ask.

Data minimisation

The data minimisation principle refers to the importance of only holding as much data about a person as is necessary. Data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. For example, if you are collecting data to post a catalogue, you only need the person's name and address. You don't need their date of birth or gender, as it's not relevant. Furthermore, when you no longer need data to fulfil its original purpose, you must securely delete or destroy it.

In accordance with this principle, you cannot collect data on a ‘just in case’ basis. You must carefully consider the purpose for which you’re acquiring data before you gather it. If you think you’ll eventually need to use a person’s data for something else, you’ll have to recollect it with new consent nearer the time. You cannot collect it in advance for future purposes.

Fulfilling the principle of minimisation is crucial for reducing risks, such as if a data breach occurs. It also ensures that data is not subject to misuse.

Accuracy

The principle of accuracy states that the data you collect must be ‘accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay’. To fulfil this principle, you must update data if a customer notifies you of a change. You must also erase the data if it’s no longer necessary. Under the regulations, data subjects have the right to rectification and you must fulfil this request within one month.

Accuracy also applies to outsourced processes, such as using an external payroll company. You must have a system in place for ensuring they can easily correct any personal data they hold. Primary data controllers are responsible for ensuring this occurs. Therefore, you must make sure you’re aware of all the third parties that process any data you hold about people.

Data retention periods

To comply with the principle of data retention periods, data you hold must be ‘kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed’. You may store it for longer for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

The duration for which you can lawfully hold data varies depending on the purpose you acquired it for. It is up to each individual business to determine this themselves. In some cases, the law may enforce a retention period. For example, you must keep P60s and P45s as part of HR records for 6 years. You should also be aware that data subjects have the right to erasure. This is also known as the right to be forgotten. If you receive a request for erasure, you must respond within a month to notify them of your intended actions.

If you no longer need data for its original purpose, or a person asks for you to erase it, you must **securely delete or destroy it**.

Another requirement regarding data retention is keeping internal records of data processing activities. This is a new requirement under GDPR. It applies to all businesses if their data processing could risk an individual’s rights or freedoms. Businesses with more than 250 employees must keep more detailed records, which the Data Protection Officer should oversee.

Data security

This is a crucial principle, as it refers to the processes you must follow to securely handle personal data. Under the regulations, it's essential that the data you hold is 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'. Data security requirements also apply to any third parties that process data you collected. It's your responsibility to ensure they comply.

Data security applies to **both physical and digital data**, and to **internal and external threats**. People must not be able to access data without proper authorisation. For example, by physically accessing a room that holds records or digitally acquiring them through cyber-attacks. Your business must have procedures in place to mitigate these risks, and it's up to you to determine what is proportionate and necessary to achieve an adequate level of security.

Examples of cyber security measures include: installing security software (such as antivirus), enforcing security policies, providing information, instruction, and training to staff, and only granting access to people who actually need to use the data.

Accountability

Accountability is a new addition to the Data Protection Act in accordance with GDPR. To comply with it, data controllers must be able to prove that their data protection measures are sufficient. They must have appropriate technical and organisational procedures, which include suitable privacy policies and keeping sufficient records of their processing activities.

Not only is accountability crucial for complying with data protection law, but it also reflects positively on your business. Customers, clients, and employees will recognise that you handle their private information securely, meaning they're more willing to give you their trust and do business with you.