GDPR has been in place since 2018 and it sets out seven main principles that underpin the very meaning of general data protection. These are set out in Article 5 of the UK and in this article, we are going to look at what they mean, enabling you to determine what GDPR means.

Lawfulness, fairness and transparency

As far as lawfulness goes, this is where specific grounds are identified in order for the handling of personal data to be lawful. This is known as a lawful basis and there are six options available that are based on your purpose and the relationship you have with the individuals. If there no lawful basis is applied, then the processing of data will be considered unlawful. Therefore, you will have to ensure you do not breach confidence, do not use your powers incorrectly, do not infringe copyright, breach a contractual agreement, breach industry specific regulations or breach the Human Rights Act 1998.

It is also important that personal data is processed fairly and that it is only handled in a way that people would consider reasonable. Therefore, it should not be used in a way that has a negative impact on them and whether you use it fairly will depend on how you obtain the data. If it was obtained through deception then it is almost going to be unfair. Understanding whether it is fair is all about understanding how it affects those concerned.

Transparency is much like fairness because it is about being honest and open about who you are and why or how personal data is used. This is crucial, particularly in instances where people can choose whether they want to have a relationship with you. If they are aware of how you will use their data from the start then they can make a decision based on their needs or expectations.

Purpose Limitation

The idea behind purpose limitation is to ensure that you are clear from the start as to why you are collecting personal data and how you plan to use it. You must also make sure that what you do with the data falls in line with the expectations of the individuals involved.

When you clearly state your purposes from the beginning, it will ensure that you are accountable for processing and ensures that individuals are aware of how you use their data, helping them to make a decision on whether they want to share their data.

When you specify your purposes, you comply with your obligations in relation to your documentation and transparency. So, you need to clearly specify your purpose which means that it is made clear that data is collected for legitimate reasons. Therefore, you have to establish clear purposes for processing data while communication is key as you will need to inform individuals via a privacy notice. You will then need to make sure you follow these purposes and make sure you stick to them. If you do have plans to use the data in another way and for another purpose then you will need to request consent.

Data Minimisation

Under this principle, you have to identify how much personal data is required in order to meet your purpose. As a result, you should only retain this information and nothing more. This principle also relates to an additional three principles for data standards as well as storage limitation and accuracy.

What you should focus on is only collecting the data that you need. You should have the ability to demonstrate that you have the correct processes in place that make it possible to only collect the data you require and hold that. Furthermore, when it comes to adequate, relevant and limited data, GDPR does not provide a definition for these and so, this will be based on how you plan to collect and use the data as this can differ from one person to another. So, in order to determine whether you are holding the right amount of data, you have to stipulate why you require it.

Finally, you should carry our periodic checks to find out whether the data you hold is still relevant and aligns with your purposes. If there is anything you no longer need then that will need to be deleted.

Accuracy

This principle links in with the data minimisation principle but there are links within this principle with the right to rectification. This enables individuals to correct any personal data that might be incorrect. Essentially, you will need to make sure that you take the right steps to

ensure that all personal data is accurate and that the personal data has a clear source and status. Should there be any information that is inaccurate, you will need to recognise the challenges associated with this but also determine whether there is a requirement to carry out periodic updates to the data.

While there is no definition of 'accurate', there is a definition for 'inaccurate' which means that you cannot mislead or provide incorrect information in relation to what you plan to include on the record of the personal data you are collecting. It is your responsibility to make sure that the data you collect and store is accurate. Therefore, you should make sure that you carry out checks to erase or update incorrect information as well as incomplete data while regular audits can help you remain compliant.

Storage Limitation

You might be lawful and fair when it comes to collecting and storing personal data but you have to make sure that you do not retain that data for any longer than it is required. So, there is a close relationship between accuracy principles and data minimisation. There are no specific time limits in place for certain types of data and so, this is down to you to determine how long you will need to keep the data for.

This is important because it will help you to comply with the accuracy and data minimisation principles. You should make sure that personal data is anonymised or erased when it is no longer required as this will help to bring a reduction in the risk that it is excessive, inaccurate or out of date. Furthermore, it will also help to reduce the likelihood that you will use this data in the correct way. If you hold personal data for too long, then it is considered to be unnecessary and you are not likely to have a lawful basis for keeping it.

Storage limitation requires good practice and the right policies in place that clearly state what retention periods should be followed. Additionally, it will help to ensure that queries about retention and erasure are easier to handle.

Integrity and Confidentiality

Collecting data and holding personal data has to be carried out in a way that maintains integrity and confidentiality. Personal data is extremely useful in the wrong hands but it is your responsibility to ensure that it is

held securely and is protected from any possible threats both internally or externally.

To achieve this, you will have to carry out the necessary planning and adopt a proactive approach to ensure that data is not processed by unauthorised individuals or unlawfully while it will also protect from damage, accidental loss and destruction. Therefore, you are expected to implement both technical and organisational measures and that includes carry out risk analysis and creating organisational policies.

Information security is crucial because it can cause distress and harm to individuals while also putting services and systems at risk. Problems such as identity fraud can arise, credit card transactions and mortgage fraud can occur as a result, so integrity and confidentiality are key.

Accountability

It is vital that you are accountable for the personal data you obtain and how you use it as well as how you adhere to other principles. It is all too easy for a business to say that they are adhering to the rules when they are not, which is why it is important that you remain accountable. Therefore, you should have the right records in place as well as measures to prove that you are compliant when it comes to the data processing principles. You might be asked for evidence at any time and that is the reason why documentation is crucial as it provides an audit trail that can be followed should you need to prove that you have acted responsibly.