| **No** | **Title** | **Principle Definition** | **Meaning of Principle (you must:-)** |
| --- | --- | --- | --- |
| 1 | Fair and lawful | Personal data shall be processed fairly and lawfully | * Have legitimate grounds for collecting and using personal data;
* Not use the data in ways that have unjustified adverse effects on the individuals concerned;
* Be transparent about how you intend to use the data and give individuals appropriate privacy notices when collecting personal data;
* Handle people’s personal data only in ways they would reasonably expect;
* Make sure you do not do anything unlawful with the data.
 |
|  |  |  |  |
| 2 | Purposes | Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. | * Be clear from the outset about why you are collecting personal data and what you intend to do with it;
* Comply with the Act’s fair processing requirements including the duty to give privacy notices to individuals when collecting their personal data;
* Comply with what the Act says about notifying the Information Commissioner;
* Ensure that if you wish to use or disclose the data for any purpose that is additional to or different from the originally specified purpose the new use or disclosure is fair.
 |
|  |  |  |  |
| 3 | Adequacy | Personal data shall be adequate. relevant and not excessive in relation to the purpose or purposes for which they are processed. | * Ensure that you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual;
* You do not hold more information than you need for that purpose.
 |
|  |  |  |  |
| 4 | Accuracy | Personal data shall be accurate and, where necessary, kept up to date. | * Take reasonable steps to ensure the accuracy of any personal data you obtain;
* Ensure that the source of any personal data is clear;
* Carefully consider any challenges to the accuracy of information; and
* Consider whether it is necessary to update the information.
 |

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | Retention | Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. | Will need to:-* Review the length of time you keep personal data;
* Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
* Securely delete information that is no longer needed for this purpose or these purposes; and
* Update, archive or securely delete information if it goes out of date.
 |
|  |  |  |  |
| 6 | Rights | Personal data shall be processed in accordance with the rights of data subjects under this Act | * Right of access to a copy of the information comprised in their personal data;
* A right to object to processing that is likely to cause, or is causing, damage or distress;
* A right to prevent processing for direct marketing;
* A right to object to decisions being taken by automated means
* A right, in certain circumstances, to have inaccurate personal data rectified, blocked, erased or destroyed; and
* A right to claim compensation for damages caused by a breach of the Act.
 |
|  |  |  |  |
| 7 | Security | Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or loss or damage to, personal data | Need to:-* Design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
* Be clear about who in your organisation is responsible for ensuring information security;
* Make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable and well-trained staff; and
* Be ready to respond to any breach of security swiftly and effectively
 |
| 8 | International | Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. | * Consider whether the personal data needs to be transferred or can it be anonymised
* If data is only in transit through a non EEA country there is no transfer outside the EEA. If personal data is added to a website based in the EU that is accessed in a country outside the EEA there will be a transfer of data outside the EEA.
* If transferring data outside the EEA you will need to comply with all the principles and the Act as a whole.
* There are no restrictions to the transfer of personal data to EEA countries.
* Transfers may be made to any country or territory in respect of which the Commission has made a ‘positive finding of adequacy’.
* Follow ICO guidance on the Privacy Shield for transferring data to the USA
 |