Data Privacy Principles

Personal data is any information about a person who can be identified, such as a name, a phone number, an email address or a photo. The European Union's General Data Protection Regulation, the GDPR, lists seven principles for handling it in Article 5. Saudi Arabia's Personal Data Protection Law, the PDPL, overseen by the Saudi Data and Artificial Intelligence Authority, follows many similar ideas. This video gives general information, not legal advice.

1. Lawful, Fair and Transparent

The first principle has three parts. Lawful means that we need a valid legal reason to use the data, such as consent or a contract. Fair means that we do not use the data in ways that people would not expect or that harm them. Transparent means that we tell people clearly what we collect, why and for how long.

Example: A gym asks members for their phone numbers. To be transparent, a sign at the desk says that the numbers are used only for class reminders, and explains how to stop them. Members feel safe and share their numbers.

At work: Afnan works in human resources at a retail company. She checks transparency and sees that the application form never tells applicants how their data will be used. She adds a short, clear notice, and applicants now know what happens to their data.

2. Purpose and Minimisation

Purpose limitation means that we collect data for a clear purpose and do not reuse it for a different purpose that does not fit the first one. Data minimisation means that we collect only the data we really need for that purpose. Every extra piece of data is extra risk if it is lost or misused. Before adding a field to a form, we can ask a simple question: do we really need this?

Example: A pharmacy loyalty card form asks for a full home address and a date of birth. Using data minimisation, the pharmacy keeps only the name and the phone number, which are all it needs for the points. The form becomes shorter, and more customers sign up.

At work: A manager asks Afnan for the files of all job applicants, just in case. She applies purpose limitation: the data was collected for one vacancy only. She shares only the shortlisted candidates for that role, and the manager gets what he really needs.

3. Accuracy and Storage Limitation

Accuracy means that personal data must be correct and kept up to date. Wrong data can lead to wrong decisions, such as a bill sent to the wrong address. Storage limitation means that we

This document is a property of Asaseeyat Academy - © Copy Right Protected.

keep data only as long as we need it for its purpose. After that, it should be deleted safely or made anonymous.

Example: A clinic keeps sending appointment reminders to old phone numbers. To keep its data accurate, the reception now asks patients to confirm their details at every visit. Reminders reach the right people, and fewer appointments are missed.

At work: Afnan finds old applicants' CVs from many years ago in a shared folder. Following storage limitation, she agrees a clear retention period with her manager. Old files are deleted safely.

4. Security and Accountability

Integrity and confidentiality mean that personal data must be protected against loss, damage and access by the wrong people. This includes passwords, access rights, locked cabinets and care when sending emails. Accountability means that the organisation is responsible for following all the principles and must be able to show it. Records, policies and training are the usual ways to prove this.

Example: A family keeps its passports and bank papers in a locked drawer, not on the kitchen table. This is confidentiality at home: only the right people can reach them.

At work: Afnan builds accountability: she writes down what personal data the team holds, why, for how long and who can see it. Only two people now have access to the salary files. When an auditor asks how the data is protected, the company can show it in minutes.

Conclusion

In summary, the GDPR names seven principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Laws such as Saudi Arabia's PDPL share many of the same ideas. In daily work, they lead to a few simple habits: tell people, collect less, keep data correct, delete it on time and protect it. For specific cases, it is always best to ask the organisation's data protection or legal team.

Sources

- Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), Article 5 – https://eur-lex.europa.eu/eli/reg/2016/679/oj
- UK Information Commissioner's Office (ICO): A guide to the data protection principles – https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/
- Saudi Data and Artificial Intelligence Authority (SDAIA): National Data Governance Platform, Personal Data Protection Law (PDPL) – https://dgp.sdaia.gov.sa/wps/portal/pdp/home
- Note: This summary is general information, not legal advice.

This document is a property of Asaseeyat Academy - © Copy Right Protected.