Key Terms

The Personal Data Protection Law No. 151 of 2020 ("PDPL") provides for specific terminology concerning personal data protection. You will find in this table a simplified definition for these terms. To allow for a clearer understanding of the personal data protection framework, these definitions follow a sequential flow rather than an alphabetical order. For more information, please visit the Frequently Asked Questions and the Checklists.

Terms	Definition
1. Personal Data	Data related to an identified or identifiable natural person, either directly or indirectly, through its association with other data such as name, voice, image, national ID number, or online identifiers, and others.
2. Sensitive Personal Data	Specific category of personal data that is considered highly sensitive and poses greater risks to an individual's privacy and security. This includes health data (psychological, mental, physical, and genetic data), biometric data, financial data, religious beliefs, political opinions, security status data, and data related to children.
3. Processing	Any activity preformed on personal data, such as collecting, storing, using, disclosing, deleting or changing it, through electronic or technological means whether partially or fully.
4. Data Disclosure	All means of enabling the knowledge of personal data to third parties, such as accessing, exchanging, publishing, transmitting, transferring, using, displaying, sending, receiving, or revealing it.
5. Controller	Any natural or juristic person who determines the purposes and means of processing personal data.
6. Processor	Any natural or juristic person who processes personal data on behalf of the controller in accordance with their instructions.
7. Joint Controllers	Two or more controllers who jointly determine the purposes and means of processing personal data.

8. Sub-processor	A separate entity engaged by the processor to carry out processing activities relating to personal data.
9. Data User	General term that covers both controllers and processors.
10. Data Subject	Any natural person to whom electronically processed personal data is attributed.
11. Data Protection officer (DPO)	An individual appointed by a data user to monitor and oversee their compliance with the PDPL, provide necessary advice on data protection matters, and act as a point of contact for data subjects and PDPC.
12. Data Protection Consultant	Any natural or juristic person accredited by PDPC as qualified to provide consultations in the field of personal data protection.
13. Recipient	Any natural or juristic person to whom personal data are disclosed from a source other than the data subject.
14. License	An official document issued by PDPC to a juristic person, granting them the authorisation to process personal data for a renewable three-year period.
15. Permit	An official document issued by PDPC to a natural or juristic person, granting them the authorisation to process personal data for a renewable period for up to one year.

16. Accreditation	An official document issued by PDPC certifying that a natural or juristic person is qualified to provide consultations in the field of personal data management and protection.
17. Lawfulness	Processing personal data based on valid legal grounds.
18. Legitimate Interest	A lawful basis for processing personal data, where the data controller's interests or those of a third party are pursued, provided these interests are not overridden by the data subject's rights and freedoms.
19. Legitimate Interest Assessment (LIA)	An assessment used to evaluate whether the processing of personal data is necessary for a legitimate interest by balancing that interest against the potential impact on data subjects' rights and freedoms.
20. Transparency /Right to be Informed	Providing the data subject with clear, accessible, and easily understandable information about how and why their personal data is being processed.
21. Privacy Notice	Notice provided by the controller that informs data subjects about how and why their personal data is being processed.
22. Internal Privacy Policy	Policy developed by an organisation to govern the processing, management, and protection of personal data within its operations. It also defines employees' responsibilities, security measures and more.
23. Fairness	Processing personal data in a way that is consistent with the data subject's reasonable expectations, without using deceptive or harmful practices.

24. Purpose Limitation	Limiting personal data collection and processing to specified, informed, and legitimate purposes.
25. Data Minimisation	Collecting only the minimal amount of personal data necessary and using the least intrusive means of processing required to fulfil the specified purposes.
26. Storage Limitation	Retaining personal data only for as long as necessary to fulfil the purposes for which they were collected.
27. Data Accuracy	Ensuring the accuracy of personal data by taking steps to keep it up-to-date and correcting any inaccuracies promptly.
28. Integrity and confidentiality	Protecting personal data from unauthorised access, disclosure, alteration, or destruction, through the implementation of the appropriate technical and organisational measures.
29. Data Encryption	A security measure that involves converting data into an unreadable format (ciphertext) using algorithms that can only be returned to its original format by using the correct decryption key to prevent unauthorised access.
30. Data Breach/Security Incident	The accidental, unlawful, or unauthorised destruction, loss, alteration, disclosure of, or access to personal data, whether in transit, storage, or processing.

31. Data Breach Register	Record containing the required information about any security breach, including the nature of the breach, its impact, actions taken in response, and whether the breach has been notified to PDPC or data subjects.
32. Accountability	Taking responsibility for personal data processed and being able to demonstrate compliance with data protection regulations.
33. Records of Processing Activities (ROPA)	Comprehensive document maintained by data users, detailing how the organisation handles each category of personal data and data subjects, including the purposes of processing, lawful basis, recipients, retention periods, security measures, and others.
34. Data Protection Impact Assessment (DPIA)	An assessment used to assess and mitigate the risks to personal data privacy and security before initiating processing activities that may impact data subjects' rights and freedoms.
35. Data Subject's Consent	A personal, informed, specific, explicit, and freely given indication of a data subject's wishes to agree to the processing of their personal data.
36. Data Subject's Rights	Set of rights granted to data subjects under the PDPL, as indicated below from definition 37 to 44.
37. Right of Withdrawal	The right that allows data subjects to revoke their previous consent to the processing of their personal data easily, in an accessible manner, and at any time.

38. Right to Access	The right that allows data subjects to request confirmation from data users as to whether their personal data is being processed by them, and if so, to obtain access to such data including information on the purposes and means of the processing.
39. Right to Rectification	The right that allows data subjects to request data users to correct any inaccuracy or complete any personal data concerning them.
40. Right of Erasure (Right to be Forgotten)	The right that allows data subjects to request data users to erase any personal data from their records.
41. Right to Object	The right that allows a data subject to stop data users from processing their personal data.
42. Right to Restriction of Processing	The right that allows data subjects to to request the temporary restriction of the processing of their personal data.
43. Right to be Informed in Case of Data Breach	The right to be notified of any data breach involving their personal data within three working days following the notification of the breach to PDPC.

44. Right to Data Portability	The right that allows data subjects to transfer their personal data from a controller to another controller.
45. Electronic Direct Marketing	The use of electronic channels, including emails, text messages, phone calls, and/or others electronic platforms, to directly promote products, services, social or political requests to data subjects.
46. Creator	Any natural or juristic person who determines the purposes and means of an electronic direct marketing communication.
47. Sender	Any natural or juristic person who transmits or delivers an electronic direct marketing communication to the data subject.
48. Opt-in	The mechanism requiring data subjects to actively provide consent before their personal data is processed or used for specific purposes.
49. Opt-out	The mechanism allowing data subjects to withdraw their consent or object to the processing of their personal data or its use for specific purposes.
50. Cross-Border Data Transfer	The transfer of personal data by a data user to another party located outside the Egyptian borders.
51. Exporter	Any natural or juristic person who, in the context of a cross-border data transfer, discloses personal data to an importer located outside the Egyptian borders.

52. Importer	Any natural or juristic person who, in the context of a cross-border data transfer, receives personal data from a data exporter.
53. Adequacy Decision	Decision made by PDPC confirming that a foreign country or international organisation ensures a level of data protection equivalent to that required under the PDPL, allowing the unrestricted transfer of personal data to that entity.
54. Binding Corporate Rules (BCRs)	Internal policies adopted by multinational organisations to ensure the safeguarded transfer of personal data within their group across borders, in compliance with personal data protection regulation.
55. Data Transfer Standard Contractual Clauses (SCCs)	Contractual clauses between data users to ensure the safeguarded transfer of personal data across borders, in compliance with personal data protection regulations.
56. Cookies	Small text files stored on a data subject's device by a website to allow the operation and management of the website, track activities, store preferences, or facilitate features such as authentication and targeted advertising.