|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ASPECTS** | **DPDP ACT** | **IS 17428\_PART-1\_2020 STANDARD** | | **ISO/IEC DIS 27701** |
| **ABOUT** | An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals (like right to be informed) to protect their personal data and the need to process such personal data for lawful purposes. | Provides specific requirements – both management and engineering - for establishing, implementing, maintaining and continually improving a Data Privacy Management System. | | This document specifies requirements for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS). |
| **PERSPECTIVE/NATURE** | Legal framework | Both Technical (SEC- 4) and Management-oriented Standard(SEC-5) | | Technical (B.3.29) and Management-oriented standard(3.23) |
| **DEFINITIONS :** |  |  | |  |
| PERSONAL DATA/INFORMATION/PII | PERSONAL DATA: Any data about an individual who is identifiable by or in relation to such data. (2.(t)) | PERSONAL INFORMATION : Any information that (a) can be used to identify the Individual to whom such information relates to, or (b) is or might be directly or indirectly linked to an Individual. (3.14) | | PII : It is the information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or might be directly or indirectly linked to a natural person. [from standard 29100, 3.7] |
| Data used to identify a specific person. | Data used to identify a specific person directly or indirectly. | | Information that is connected to a specific person directly or indirectly. |
| DATA or PII FIDUCIARY/CONTROLLER | “Data Fiduciary” means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data. (2.(i)) | “Data Controller” means any organization that determines the means and purposes of processing the personal Information. (3.3) | | PII controller is the one who determines the purposes and means of the processing of PII. [from standard 29100, 3.7] |
| An individual or organization that decides how and why personal data is collected and used. | An individual or organization that decides how and why personal information is collected and used. | | The person or entity that decides why and how PII is collected and used. |
| DATA/PII PROCESSOR | Any person who processes personal data on behalf of a Data Fiduciary. (2.(k)) | Any organization that processes personal information on behalf of and in accordance with the instructions of a data controller. (3.5) | | PII PROCESSOR : Privacy stakeholder that processes PII on behalf of and in accordance with the instructions of a PII controller. [from standard 29100, 3.10] |
|  |  | | An entity that handles PII as directed by PII controller.  Section 7 in 27701 does not explicitly contains the definition of data processor, however, it provides a framework for data processors to establish, implement, and maintain a robust privacy information management system, which is crucial for their operations and compliance. |
| DATA PRINCIPAL/DATA SUBJECT | Data Principal - The individual to whom the personal data relates. (2.(j)) | Data Subject - Any natural person to whom the personal Information relates. (3.6) | | PII PRINCIPAL:  A natural person to whom the PII relates  [from standard 29100, 3.9] |
| The person whose data is being collected. |  | | The person whose data is being collected. |
| CONSENT |  | Data subject’s freely given, specific and informed agreement to the processing of their personal information. (3.2) | | PII’s freely given, specific and informed agreement to the processing of their PII [from standard 29100, 3.4] |
| Not mentioned explicitly. | It's when a person agrees to let their personal information be used, after being fully informed about how it will be processed and for what purposes. | | It's when a person agrees to let their PII be used, after being fully informed about how it will be processed and for what purposes. |
| SENSITIVE PERSONAL INFORMATION |  | A special category of personal information, whose nature is either sensitive or that might have a significant impact on the individual. (3.22) | | Category PII either whose nature is sensitive, such as those that relate to the PII Principal’s most intimate sphere, or that can have a significant impact on the PII principal. [from standard 29100, 3.23] |
| Not mentioned explicitly. | It's a type of personal information that's considered more private or vulnerable, such as political opinions, or biometric data. | | It's a type of personal information that's considered more private or vulnerable, such as political opinions, or biometric data. |
| PRIVACY CONTROLS |  | The measures that protect personal or sensitive personal information by reducing the likelihood of occurrence of privacy risk. (3.16) | | Measure that treats privacy risks by reducing their likelihood or their consequences. [from standard 29100, 3.12] |
| Not mentioned explicitly. | These measures reduce the occurrence of risks to (sensitive) personal information. | | These measures reduce the occurrence of risks. |
| PRIVACY RISK ASSESSMENT | Periodic Data Protection Impact Assessment - A process comprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals. (Pg no. 9) | It is the overall process of risk identification, risk analysis and risk evaluation with regard to the processing of personal information.(3.17) | | It is the overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of PII framed within an organization’s broader risk management framework. [from standard 29100, 3.18] |
| A method to protect people's rights, and manage risks when handling personal information. | A process to identify and address potential privacy risks when handling personal information within an organization. | | A process to identify and address potential privacy risks when handling personal information within an organization. |
| SECONDARY USE |  | Constitutes processing of personal information in conditions which differ from the primary use initially communicated to or agreed with the individual.(3.21) | | Use of data for additional purposes than the primary reason for their collection, adding value to this data.  [from ISO/TR 22221:2006, definition 2.16(OBP)] |
| Not mentioned explicitly. | Secondary use is using personal data for purposes beyond what was originally agreed upon by the individual. | | Using the data collected for purposes beyond its original intent. |
| Processing | “Processing” in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage etc. (2.(x)) | | Processing — Any operation or set of operations performed upon personal information, whether or not by automatic means.(3.18) | It is an operation or set of operations performed upon PII. [from standard 29100, 3.21] |
| Processing is any action performed on digital personal data. | | Processing is any action performed on digital personal information. | Processing is any action performed on PII. |
| **REQUIREMENTS** |  | |  |  |
| a) CONSENT & NOTICE - |  | |  |  |
| ii) CONSENT REQUIREMENT | Free, specific, informed, unconditional, unambiguous. (6.(1), pg no. 5) | | When consent is the lawful basis, obtain lawful and fair consent.(4.2.3) | Specific to purpose ( B.1.2.4) and it should be according to the documented process  (Pg no. 16) |
| ii) NOTICE REQUIREMENTS | Clear notice with specified purpose and content (5.(1), pg no. 4) | | Privacy notice with specified content (4.2.2) | The organization shall provide PII principals with clear and easily accessible information (notice) identifying the PII controller and describing the processing of their PII (A.1.3.4, Pg no. 17) |
| iii) Language | Option to access in English or languages in 8th Schedule (pg no. 5) | | Not Specified. | Clear and plain language can be used. (B.1.3.4) |
| b) DATA COLLECTION AND USE |  | |  |  |
| i) PURPOSE LIMITATION | Specified purpose. (6.(1), pg no. 5) | | Use only for legitimate and agreed purposes (4.2.4) | The organization must process personal data only for purposes explicitly specified by the customer in their documented instructions. (B.2.2.3) |
| c) DATA SECURITY | Implement reasonable security safeguards (the schedule - table) | | Adopt and implement information security program (4.2.6) | Requires appropriate security controls (6.1.3 ©) |
| d)ACCOUNTABILITY (taking responsibilit-y to demonstrat-e data protection principles) | Data Fiduciary processes the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose (4.(1), pg no. 4) | | Establish and document a Data Privacy Management System (DPMS) that acts as a baseline and reference point for determining the data privacy requirements for the organization (5.3) | Assigns responsibility and authority for ensuring PIMS conformity and performance reporting to top management (5.3) |
| e) RISK MANAGEMENT | Requirements for Data Protection Impact Assessments and periodic audits ( 2©, pg no. 9) | | Establish privacy risk management methodology (5.8) | Establishes and maintains privacy risk criteria and the organization shall define and apply a privacy risk treatment process to treat risks related to the  processing of PII (6.1.2) |
| f) CONTINOUS IMPROVEM-ENT | Not Specified. | | Implement a documented process for measuring and continuously improving the DPMS(5.15) | The organization is required to continually improve the suitability, adequacy and effectiveness of the privacy information management system (10.1) |