DGPSI-HR

30 Implementation specifications of DGPSI-HR

MIS No	Description of the Implementation Specification
1	Organization shall designate a **Compliance Manager**, with necessary credentials and provide support in terms of people, budget and technology and external consultancy. Organization shall constitute **the Data Governance and Data Protection committee** represented by all internal stake holders, the Chief HR manager, the designated Compliance officer with one of the directors as the Chair person. The committee shall adopt a **comprehensive Data Processing Policy** inclusive of all data protection related recommendations including representing a fair valuation of data and monitor their compliance from time to time. The committee shall also cause data audits to be conducted from time to time under the supervision of the Compliance officer and review it at periodical intervals with periodical external validation.
2	Organization shall create an Inventory of all processes that process personal data on related to is HR operations. The inventory shall have a unique ID, a process owner, identified purpose, required data elements, required storage, identified persons who access the data The lifecycle of data includes receipt of data, prospecting, background verification, onboarding, evaluation, reward and sanctions, termination and post termination and incorporate multiple processes in the life cycle. Processes such as welfare schemes, Insurance and other welfare schemes to the employee or his family, logistics services, travel services, Visa services etc shall also be considered as specific processes to be covered under the Compliance program.
3	Organization shall create an inventory of all personal data processed in relation to the HR operations linked to each process. This inventory will contain a master ID for each data set, multiple data elements under each set with subgrouping flagged to different processes. Data sets may also be tagged with specific tags related to classification for the purpose of compliance so that controls can be implemented effectively.
4	All contract employees, consultants, and outsourced personnel engaged by the Organization who have access to or process Personal Data shall act under the authority of the Organization and shall be bound by written confidentiality, security and data-protection obligations aligned to the Digital Personal Data Protection Act, 2023 (DPDPA). Where a consultant or service provider independently or jointly determines the purposes and means of processing Personal Data, such party shall be treated respectively as a Data Fiduciary or Joint Data Fiduciary for that processing
5	Where the Organization supplies its employees to another organization and such personnel process Personal Data under the instructions of the recipient organization, the recipient organization shall be considered as the primary Data Fiduciary. The supplying Organization to which the individual worker has "Employment" obligations shall be considered as jointly determining the means of processing and hence both organizations shall be considered as data fiduciaries. The Organization supplying personnel shall ensure project specific back-to-back contractual obligations with such personnel, including confidentiality, security and

	lawful-processing duties, aligned with its obligations under any Data Processing or Joint Data Fiduciary agreements.
6	Where the personnel supplied by the Organization are not employees but are on contract themselves and such personnel process Personal Data under the instructions of the recipient organization, the supplier organization may be only supplying a contract worker and hence could be a Data Processor. The contract employee himself may be an individual joint data fiduciary or a data processor of the resource receiving organization depending on the scope of engagement. The Organization supplying personnel shall ensure project specific back-to-back contractual obligations with such personnel, including confidentiality, security and lawful-processing duties, aligned with its obligations under its business to business agreement.
7	Organization shall conduct periodic awareness of the legal provisions of the Act including the duties of the data principal, and skills training required to implement the policies of the organization under the distributed responsibility principle. The "Awareness" needs to be supplemented with "Acceptance" through appropriate ethical assurance.
8	Each process shall be supported by a documented legal basis policy including exemption policy or legitimate use or Consent policy as per the provisions of the DPDPA. Where the purpose can neither be supported by an exemption provision or a legitimate use provision, appropriate consent management shall be tagged for establishing the legal basis.
9	Each process for which consent is required and obtained shall be supported by a distinct privacy notice with appropriate language options and specified content as per the act and the rules including need to identify before exercising of any rights on a later date. One consent for multiple purposes shall be avoided.
10	Organization shall ensure that special consents are obtained where processing of biometrics or other forms of sensitive information is processed or where the provision is considered unclear under law. Such special consent may document an explicit explanation and witnessed.
11	Privacy Notices shall be issued and maintained to all current and past employees whose personal data is in use by the company. Where approved consents are not received back within a reasonable time or rejected, the Governance Committee shall review and document its decision to use legitimate use and archive the after due notice to the data principal. Where the company is in the possession of personal data which is no longer in use, and are not required to be retained, they shall be purged with suitable documentation.
12	All consents and any modifications thereof shall be adequately authenticated and preserved with a unique tracking ID for such period as is required under law. Where the retention is not related to the current processing requirement, the information shall be securely archived
13	Organization shall ensure appropriate policies and procedures are in place to protect the **rights of the data principal** such as Right to Access, Right to Correction and Erasure,

	Right to Grievance Redressal and Right to Nomination as well as the Rights of minor or mentally disabled persons.
14	Organization shall Establish procedure for using consents received from a Consent Manager with appropriate safeguards to protect the confidentiality of internal information. DGPSI recommends that Employee consents need to be direct and not through Consent Managers Conflicts if any are to be resolved as grievances
15	Where third party service providers are used for any process, the organization shall ensure that the contract specifies the obligations including whether the contractor is a joint data fiduciary and accepts audit and security clauses. Where shared platforms are used for background verification or cloud storage or any other purpose, care shall be taken that special safeguards are in place to secure the wrongful disclosure of data
16	Organization shall Ensure keeping track of any directions from the regulatory authorities including sectoral regulators about restrictions for personal data transfer outside India
17	Organization shall Ensure protection of personal data with self and with data processor with reasonable security safeguards commensurate with the nature and sensitivity of the personal data processed including use of techniques such as Pseudonymization, anonymisation, tokenization, Encryption, Access control, CIA protection and data leakage prevention, Appropriate log management
18	Organization shall Establish appropriate policy to identify, investigate, respond and report a personal data breach to the DPB/Data Principal and any other statutory authority as may be required under applicable law as required.
19	Organization shall Publish the business contact information of the DPO/Compliance officer on the public website, on any interfaces where personal data is collected and all Privacy Notices. Accountability for business contact email addresses in the name of an impersonal "designation" or "function" are at all times with a designated human and a confirmation to that extent shall be published along with the Business Contact.
20	Where the processing occurs outside the Indian geography, appropriate measures to meet the restrictions on cross border transfer if any shall be in place.
21	Organization shall Establish measures to promptly receive and respond to any communication received from the Data Protection Board, participate in the inquiry process and avail of the voluntary undertaking benefit where available. Where necessary systems should be in place to consider timely appeals and proper representation in the hearings.
22	Organization shall establish an appropriate policy to identify, assess, document and manage AI risks in its own processing operations as well as processing with data processors, and obtain appropriate assurances from the developers of the algorithms and or the vendors. .

23	Organization shall establish an appropriate policy to ensure that there is an accountable human handler in the organization as well as in the AI vendor organization and AI deploying data processor organization
24	Organization shall adopt AI deployment based on documented business justification, risk assessment and approval
25	Organization shall ensure that an acceptable use policy for IT assets are instituted for all IT Assets as well as AI usage.
26	Organization shall consider the Data Assets issued to employees including corporate emails or laptops or mobiles for official use as the assets of the organization and an explicit acknowledgement is held on records with an obligation to responsibly secure the data and return them at the time of termination.
27	Organization shall ensure that the compliance activities are suitably documented including log records which shall be retained as required under law
28	Organization shall establish and maintain documented policies, procedures and governance mechanisms to ensure compliance with the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 and related Rules, while ensuring protection of personal data and confidentiality of complaint handling processes in conformity with DPDPA 2023.
29	Organization shall establish and maintain documented policies, procedures and accountability mechanisms to ensure compliance with the Information Technology Act, 2000, applicable Rules, CERT-In Directions and other legal requirements relating to electronic records, electronic communications, cyber incidents and information systems while ensuring consistency with DPDPA 2023.
30	Where the Organization is a Public Authority or is otherwise subject to statutory transparency obligations, the Organization shall establish and maintain documented record management, information disclosure and governance procedures to ensure compliance with the Right to Information Act, 2005 while balancing transparency obligations with privacy and confidentiality requirements under DPDPA 2023 and other applicable laws.