18 principles of DGPSI and DGPSI-AI

The 12 principles of DGPSI- Full version are as follows:

No	Principle	Explanation
1	Process is the Focus	Under this principle, every process with a specific "purpose" involved in DPD(DPDPA Protected Data) processing is identified as the unit of compliance. The "Purpose" is derived from the business objectives and broken down under the principle "One Purpose-One Process". This helps in identifying the minimal data required, data retention required, data access requirements etc.
2	Classification is the key	Different types of data require different compliance requirements. For example, minor's data requires parental consent while data required for legal defence requires a legitimate use support. These different compliance requirements are better managed if data is classified and segregated into multiple bins with each bin containing a type of data. Assigning of controls to each such set becomes easy.
3	Hybrid Entity Concept	Segregation of the enterprise business into multiple processing activities on "One purpose-One process" basis automatically provides for accounting some processes in which the company may be a data fiduciary and in some significant data fiduciary and in some only a data processor. Today, the law classifies an entity as a data fiduciary or data processor or a significant data fiduciary at the entity level. But DGPSI recognizes that once processing is segregated, we will have some processes where the entity does only a Data Processor's job either for an internal

		department or an external entity which takes the responsibility for determining the purpose and means. The hybrid entity concept enables risk reduction within different processes so that only such processes where the risks are higher gets classified as "Significant Data Fiduciary"
4	Distributed Responsibility	This principle envisages that the responsibility for compliance internally in an organisation is distributed with the people closer to the process. Every process owner is an effective compliance manager. Alternatively, every process will have a "Process Manager"
5	Data Has Monetary Value	This principle suggests that Data as an asset must be recognized with a monetary value. It recognizes the fact that Data during its lifecycle changes in value and the change of value of data is also the cost of production.
6	Measurability	This principle recognizes that "Compliance" should be measurable. Though legal compliance is subjective, it has to be reasonably converted into an objective measurable parameter for better monitoring.
7	Critics are early whistle blowers	This principle recognizes that the Incident Management system starts with the identification of a potential risk and the early indication of an incident comes from a complaint either from within the company or from a customer or a vendor. This needs to be recognized incentivised and explored.
8	Top Management Responsibility	This principle recognizes the need of the top management to be involved in the compliance. The top management includes all the stake holders including Marketing, HR and Finance along with the legal, Technical and Research divisions.
9	Business Level Implementation	This principle recognizes that compliance system has to be integrated with the entire business cycle and not limited to the

		processing cycle. Hence acceptance of Vendors, Customers etc or purchase or sale of assets, corporate decisions like mergers and acquisitions are all part of compliance radar
10	Documentation	This principle underscores the need for documentation for the purpose of accountability.
11	Security	This principle keeps the normal requirements of preserving the confidentiality, Integrity and availability as well as prevention of data leaks as part of the compliance responsibility
12	Motivation	This principle recognizes the importance of humans who need to implement other Technical, Legal and Governance measures

Summary of Six Principles of DGPSI_AI

DGPSI-AI Principle-No	Principle
1	Unknown Risk is a Significant Risk
2	Behind every AI algorithm there shall be one human for accountability
3	Every Privacy Notice covering an AI Process involved in processing of personal data shall be accompanied by an Explainability disclosure.
4	Use of every AI Process shall be validated by a document justifying the technical, operational and economical need both at the level of the Data Fiduciary and the Data Processor with unconditional indemnity to the data principal.
5	Every AI process shall document the specific guardrails to secure the processing against Dark Patterns, Neurological manipulation and physical harm to any data principal.
6	The responsibility of the AI deployer as a "Fiduciary" shall ensure all measures to safeguard the society from any adverse effect arising out of the use of the AI.

With DGPSI-AI for DPDPA Compliance in an AI Environment

50 Model Implementation Specifications of Full DGPSI Framework

[P.S: Lead Responsibility levels (LRL):

M=Management, D=DPO, H=HR, L=Legal, T=Technology]

No MISF	Description of Specifications	LRL
	MANAGEMENT (15)	
1	Organization shall designate/appoint DPO/Compliance Manager, with necessary credentials and provide support in terms of people, budget and technology and external consultancy.	M-1
2	Organization shall constitute the Data Governance and Data Protection committee under the chairmanship of a Board member, preferably an independent director, Designated DPO/Compliance officer as the Secretary and representation of key stakeholders such as the CEO,CFO, CMO CTO, CISO, Chiefs of Legal, HR.	M-2
3	Organizations which are Significant Data Fiduciaries shall appoint an independent external Data Auditor with necessary credentials.	M-3
4	All policies shall be subject to "Exceptions" and the Organization shall establish an appropriate exception handling policy and procedures with adequate checks and balances with appropriate documentation.	M-4
5	Establish a policy of distribute responsibility for data protection where every employee will be responsible for data protection within their domain of control of data.	M-5
6	Organization shall conduct a business impact assessment to determine the applicability of data protection laws to its	M-6

	operations with reference to the type of data processed, the volume and nature of processing and status as a data fiduciary, Significant Data Fiduciary.	
7	Organization shall establish an appropriate policy for applying "Legitimate Use" provisions as legal basis for processing personal data including publicly available data, Anonymized personal data, personal data of data principals outside India etc.,	M-7
8	Organization shall establish an appropriate policy for identifying and availing Exemptions available under the data protection laws where available	M-8
9	Organization shall establish an appropriate policy to recognize the financial value of data and assign a notional financial value to each data set and bring appropriate visibility to the value of personal data assets managed by the organization to the relevant stakeholders.	M-9
10	Organization shall establish an appropriate policy for identifying and factoring the impact of data protection laws at all levels of business operations commencing from marketing of new business and through the data processing lifecycle.	M-10
11	The organization shall establish appropriate policy for using services of third-party contractors for data processing and enter appropriate enforceable contractual agreement with appropriate assurances towards data protection. Such contracts shall also enable audits and indemnities as may be required and cover all services related to personal data processing including manpower outsourcing, cloud services, shared services for hosting of website, e-mail, application development etc.	M-11

12	Organization shall establish a system for monitoring and managing the relations with regulatory agencies such as DPB, CERT IN and other sectoral and jurisdictional regulators.	M-12
13	Organization shall establish a Policy for Data Monetization in a manner compliant with law.	M-13
14	Organization shall establish an appropriate policy for maintaining digital presence on the web, mobile, Wearables, IoT etc with adequate security against misuse of applicable data protection laws including intellectual property and cyber crime laws.	M-14
15	The Organization shall establish policy for conducting a risk assessment identifying risks of non compliance under all applicable data protection laws including laws such as ITA 2000, establish a risk management strategy, to issue an implementation charter for compliance.	M-15
DPO (17)		
16	Organization shall establish an appropriate policy for continuing use of legacy personal data and for continuing use of personal data after the end of the purpose for which it was collected. Such policy shall include sending of notice, monitoring and documenting the response and initiating necessary follow up actions.	D-1
17	Organization shall establish appropriate policy for Internal and External Data Audit including DPIA, Audit of Data Processors/Business Associates, Audit of suspected data breach incidents etc.	D-2
18	Organization shall establish appropriate policy to issue privacy notice based on the Context and purpose. Such	D-3

	policies shall include appropriate policies for web or mobile or other applications.	
19	Organization shall establish an appropriate policy for minimization of data collection based on purpose in each process.	D-4
20	Organization shall establish an appropriate policy for minimization of data retention based on the purpose and in compliance with retention requirements under applicable laws.	D-5
21	Organization shall establish an appropriate policy for keeping personal data updated, to maintain the completeness, accuracy, and relevancy as per all applicable laws.	D-6
22	Organization shall establish an appropriate policy for Identifying end of purpose of collection of any personal data or withdrawal of consent and initiating necessary action of deletion, archival, or anonymisation.	D-7
23	Organization shall establish an appropriate policy for managing relationship with Consent Managers including setting up technical measures for receiving and withdrawing consent or for exercising any rights of the data principal.	D-8
24	Organization shall establish an appropriate policy for handling unstructured personal data including discovery, merging with other structured collection of personal data, erasure in unstructured form etc.	D-9
25	Organization shall establish an appropriate policy for providing "Access" rights to data principals including verifiable identification	D-10
26	Organization shall establish an appropriate policy for providing Right to Correction to data principals including verifiable identification	D-11

27	Organization shall establish an appropriate policy for incident management in the context of Privacy with relevant incident identification, incident validation and incident management.	D-12
28	Organization shall establish an appropriate policy for data breach notification for timely recognition and notification to all stakeholders under data protection laws, other laws such as ITA 2000 or sectoral regulations or the law enforcement authorities as may be required. The policy shall include measures to be undertaken from time to time for prevention, and detection of privacy incidents and corrective measures.	D-13
29	Organization shall establish an appropriate policy for disclosure and destruction of personal data as per all applicable laws.	D-14
30	The Organization shall establish an appropriate policy for implementing security measures at different levels such as Physical, logical, application or data level access required to protect unauthorized access to personal data assets whether they are located in the organizational resources or with data processors or cloud operators or employees.	D-15
31	The Organization shall establish an appropriate policy for acquisition or disposal or sharing or licensing of hardware and software assets from reliable and verified sources with assurance on security.	D-16
32	The Organization shall establish an appropriate policy for documentation of all compliance activities	D-17
LEGAL (5)		
33	Organization shall establish an appropriate policy for providing "Nomination" facility to data principals including	L-1

	verifiable identification of the nominee and description of the data assets to which nomination is applicable.	
34	Organization shall establish a policy for handling personal data of data principals "Reported Deceased" including verification of a report of death of a data principal, notification to a nominee, processing the nominee's request, resolving objections of other legal claimants etc.	L-2
35	Organization shall establish a policy for providing an appropriate Grievance redressal mechanism for data principals and other stake holders during the entire life cycle of the dispute resolution including complaint, appeals and resolution.	L-3
36	Organization shall establish an appropriate policy for collection and verification of status of a minor or other disabled data principals who are represented by legal guardians and to manage such consent along with restrictions such as behaviour monitoring or targeted advertising as well as transmission of consent control back to the minor/disabled person on termination of the power of the guardian.	L-4
37	Organization shall establish an appropriate policy for structuring contracts with business associates as instruments of ensuring compliance. Such policy shall ensure updating for data protection requirements, identifying inter-se responsibilities, contact persons, expiry etc.	L-5
HR (5)		
38	Organization shall maintain an inventory of people with relevant policy for assigning responsibility under distributed responsibility, providing privacy awareness training on a periodical basis.	H-1

39	Organization shall establish an appropriate Privacy policy for processing personal data of employees, including those who are in the recruitment process or have ceased to be employees, or working on manpower supply contracts, as per applicable laws.	H-2
40	Organization shall establish an appropriate augmented HR Policy for developing a Compliance Culture in the organization including imposition of duties, sanctions and incentives.	H-3
41	Organization shall establish a whistleblower policy covering employees and extending to external participants including the public with appropriate witness protection and incentives.	H-4
42	Organization shall establish an appropriate accepted usage policy of resources allocated by the organization including in the context of working from locations outside the office and using Own Devices with relevant sanctions for violation.	H-5
TECHNOLOGY (8)		
43	Organization shall develop an Inventory of Processes, which generate, Use, Disclose or Destroy Personal Data with unique process ID assigned to each process and tagging the purpose of processing.. Each process shall also identify and tag the contextual role of the organization as Data Fiduciary, Data Processor or Joint Data Fiduciary. Each Process shall identify a process owner who shall as an Internal Data Controller be responsible for compliance within his area of operation.	T-1

	Each process shall identify the input output data, nature of processing, storage status and movement of data during processing and storage. Each process shall adopt dynamic access permissions on a need to know basis. Each process shall tag the restrictions on the rights of use as per contractual permissions covering data protection laws, IPR laws, sectoral regulations etc.	
44	Organization shall create an inventory of personal data as a data set with a unique Master Data Management (MDM) with necessary attributes. The attributes shall include the source of the data and the legal basis of collection. Each personal data set shall be associated with classification attributes such as Minor, Employee, Sensitive, applicable jurisdiction etc. Organization shall establish a technology architecture that creates an inventory of personal Data Identifiers, and run continuous search for periodical updating, merger, de-duplication, and classification of data as personal data as combinations of data identifiers. Organization shall identify a unique ID as a Core ID associated with the MDM ID and establish a system for populating other personal data attributes on an ongoing basis	T-2
45	The Organization shall set up an appropriate policy for use of Pseudonymization, anonymization and data masking for secure disclosure of personal data between processes or for disclosure.	T-3

46	The organization shall create a Centralized Personal Data Store and secure remote access architecture with virtual processing.	T-4
47	The Organization shall establish an appropriate set of information security controls necessary for protecting the data prevention of unauthorized access, modification or denial of access applicable to personal data and also data leakage and data exfiltration along with Shall include policy for using encryption in storage, transit, processing along with required key management system. Shall include data integrity management and non-repudiable authentication of data with the use of appropriate techno legal tools. Shall also include system updating and malware etc.	T-5
48	The Organization shall establish an appropriate policy for handling transit of data across jurisdictional borders as per applicable law including sectoral laws	T-6
49	The Organization shall establish an appropriate policy for disaster recovery and Business Continuity to meet requirements during exigencies. Shall include escrow of encryption keys, critical software code etc. where appropriate.	T-7
50	The Organization shall establish an appropriate policy for adopting technical measures to segregate processing of personal data of different jurisdictions and to maintain arm's length relationship between service units belonging to different jurisdictions.	T-8

Note:

1. All policies which follow the requirements above need to be supported with detailed operational procedures, communicated to employees, awareness

created, and monitored for proper implementation. The word "Appropriate" with respect to policies indicate that they are based on suitable risk identification and assessment with an objective of mitigating the risks to the threshold level of risk absorption capability of the organization.

2. The above implementation specifications are considered the "Requirements" suggested as "Model". Organizations may through appropriate risk assessment and a considered risk management strategy create a "Deviation Justification Document" and defer adoption and/or modify of some of the implementation specifications and create an "Implementation Charter" for the purpose of implementation.

Nine Model Implementation Specifications of DGPSI-AI for Deployers

Following is the list of suggested Nine Model implementation specifications under DGPSI AI for deployers who are data fiduciaries under DPDPA.

MIS-AI No	Specification
1	The deployer of an AI software in the capacity of a Data Fiduciary shall document a Risk Assessment of the Software obtaining a confirmation from the vendor that the software can be classified as 'AI' based on whether the software leverages autonomous learning algorithms or probabilistic models to adapt its behaviour and generate outputs not fully predetermined by explicit code. This shall be treated as DPIA for the AI process.
2	The DPIA shall be augmented with periodical external Data Auditor's evaluation at least once a year.
3	Where the data fiduciary in its prudent evaluation considers that the sensitivity of the "Unknown Risk" in the given process is not likely to cause significant harm to the data principals, it shall create a "AI-Deviation Justification Document" and opt not to implement the "Significant Data Fiduciary" obligations solely as a reason of using AI in the process.
4	Designate a specific human handler on the part of Deployer-Data Fiduciary to be accountable for the consequences of the use of AI in personal data processing. By default the DPO/Compliance officer will be accountable. However, the "Process Owner" envisaged under the DGPSI framework and Process based compliance could be an alternate designate.
5	Document the human handler for the AI on behalf of the licensor through the licensing contract and if the developer has hardcoded the accountable person for the AI in the Code, the same may be recorded in the licensing contract.
6	The deployer shall collect an authenticated "Explainability" document from the developer as part of the licensing contract indicating the manner in which the AI functions in the processing of personal data and the likely harm it may cause to the data principals.
7	The deployer shall develop a "AI Justification Document" before adopting an AI led process for processing personal data coming under the jurisdiction of DPDPA justifying the use of AI and exposing the data principals to the unknown risks from technical and economical perspectives.
8	Document an assurance from the licensor that

	1. the AI software is adequately tested at their end for vulnerabilities, preferably from the third party auditor. The document should state that the "When deployed for data processing, the AI Software is reasonably secured against vulnerabilities that may adversely affect the confidentiality, integrity and availability of data and the Privacy principles where the data processed is "Personally identifiable data". 2. The document shall also mention that sufficient guard rails exist to protect the Data Principals whose data may be processed by the deployer. 3. The document shall also mention that the AI has been tested and is free from any malware that may affect other systems or data owners.
9	The Deployer of an AI shall take all such measures that are essential to ensure that the AI does not harm the society at large. In particular the following documentation of assurances from the licensor is recommended. 1.The AI comes with a tamper-proof Kill switch. 2.In the case of Humanoid Robots and industrial robots, the Kill Switch shall be controlled separately from the intelligence imparted to the device so that the device intelligence cannot take over the operation of the Kill Switch. 3.Where the kill switch is attempted to be accessed by the device without human intervention, a self destruction instruction shall be built in. 4.Cyborgs and Sentient algorithms are a risk to the society and shall be classified as Critical risks and regulated more strictly than other AI, through an express approval at the highest management level in the data fiduciary. 5.Data used for learning and modification of future decisions of the AI shall be imparted a time sensitive weightage with a "Fading memory" parameter assigned to the age of the observation. *6. Ensure that there are sufficient disclosures to the data principals about the AI risk*

36 Implementation specifications of a simplified version of DGPSI-Lite meant for SMEs

MIS-L No	Description of the Implementation Specification	DPDPA Section
1	Establish whether the organization is processing personal data for a lawful purpose to which DPDPA is applicable and whether the organization is determining the Purpose and/or Means of processing.	**4**
2	Establish the legal basis as "Consent" or "Legitimate Use" for each process.	**4**
3	Develop appropriate Notice/s indicating types of data collected, the purpose of collection with details of when the purpose terminates and how the data collected is related to the purpose.	**5**
4	Notice should indicate manner of exercising of Rights by Data Principals including power to withdraw consent, with a reminder of the duties of the data principal and consequences of withdrawal of consent	**5**
5	Notice should indicate manner of making complaint to DPB.	**5**
6	Notice should inform the availability of and manner of invoking the Grievance redressal mechanism.	**5**
7	Notice should be available in 22 Scheduled Indian languages with an option for the data principal to chose.	**5**
8	Obtain consent which is Free, Specific, affirmative action, signifying agreement, (*Generate the inventory of Personal Data with unique Consent tag)*	**6**
9	Establish procedure for using consents received from a Consent Manager	**6**
10	Ensure documenting of the consent for prospective collection of personal data and tagging it with the relevant data set. *(Multiple notices and consent formats are required for multiple sources of collection)*	**6**
11	Ensure sending of notice to data principals of legacy holding of personal data, obtain consent and follow up for	**6**

	recording rejections, non-delivery, acceptances and no response. *(Requires discovery of personal data in the organization and its Data Processor's control)*	
12	Establish policy for legitimate use of personal data, with monitoring and control. *(Needs validation from the Top Management)*	**7**
13	Ensure that the systems are in place to enable compliance with all aspects of the Act including the new the notifications that may be issued from time to time. (from MEITY/DPB or sectoral Regulators) *(The Data Fiduciary concept imposes a responsibility for compliance in letter and spirit)*	**8**
14	Ensure availability of appropriate contract for all downstream data processors and also with upstream vendors. *(Requires systematic review of every business contract)*	**8**
15	Establish appropriate technical and organizational measures for effective observance of compliance. *(This is an open ended and dynamic requirement and related to a risk assessment)*	**8**
16	Ensure protection of personal data with self and with data processor with reasonable security safeguards. *(This is an open ended and dynamic requirement and related to the preservation of confidentiality, integrity and availability of subject personal data.)*	**8**
17	Establish appropriate policy to identify, investigate, respond and report a personal data breach to the DPB/Data Principal. *(Requires an appropriate Incident Identification, Reporting, evaluation and response system)*	**8**
18	Ensure data retention is linked to purpose of collection. *(Requires erasure or archival of data when the purpose is terminated or consent withdrawn)*	**8**
19	Publish the business contact information of the DPO/Compliance officer.	**8**
20	Establish an appropriate Grievance Redressal mechanism.	**8**

	(Requires a responsive complaint handling system with negotiation, intervention of ombudsman and mediation)	
21	In case of minors or persons with disability to provide own consent, obtain verifiable consent from the parent or guardian. *(Requires age-gating and identification of data principals to whom the tag of minor or disabled can be applied)*	**9**
22	Establish policies to restrict the behaviour monitoring or targeted advertising of the minor. *(Requires management of activities of Advertisers)*	**9**
23	Identify if the organization is a Significant Data Fiduciary (SDF) and document the reasons thereof. *(Err on the safe side)*	**10**
24	If organization is a SDF appoint a Data Protection Officer with relevant credentials. *(Requires understanding of what is required to be a good DPO in India. A qualification in GDPR compliance is not necessarily a qualification in DPDPA. It may be a good practice to retain access to external DPO consultants to meet exigencies to assist the DPO)*	**10**
25	If organization is a SDF, appoint an independent Data auditor with relevant credentials.	**10**
26	If organization is a, SDF, establish a policy for conducting periodic Data Protection Impact Assessment and Periodic audit for relevant processes.	**10**
27	Establish measures to provide right to access to a data principal and to respond promptly with appropriate response. *(Note that if any adverse information has been hidden in the notice, it may get revealed in the summary of processing to be revealed)*	**11**
28	Establish measures to provide right to correction and erasure, to a data principal and to respond promptly with appropriate response. *(Note that the data principal has a duty to provide correct information and correct wrong information if already held)*	**12**
29	Inform and educate the Data Principal on the existence and use of grievance redressal mechanism and its access through the consent manager.	**13**

30	Establish appropriate measures to provide right to nomination and necessary measures to act there on at the appropriate time. (This requires an elaborate system of claims management)	**14**
31	Ensure that the data principals are appropriately informed about their duties under the Act. *(It would be a good practice to obtain an undertaking)*	**15**
32	Ensure to keep track of any directions from Data Protection Board or relevant sectoral regulators about restrictions for personal data transfer outside India.	**16**
33	Establish appropriate measures to identify and avail exemptions available with strict observance of attached conditions and limitations. *(Note that all exemptions have their own individual limitations, and a strict adherence is required)*	**17**
34	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.	**28**
35	Establish measures to receive directives from Data Protection Board and respond appropriately and without delay to comply with the order or otherwise respond to it with appeal, or representation for review or for proposing voluntary undertaking	**30**
36	Establish measures to structure and propose voluntary undertaking where required	**32**

13 Implementation Specifications for DGPSI-AI to be mandated by Deployers on the AI Vendors

MIS-No (DGPSI_AI-Developer)	Description
1	The AI developer shall generate an "Explainability" document for the AI that explains the Algorithmic function of the Model embedded in the software using the key principles of transparency as per enclosed format. (refer footnote)
2	The AI developer shall provide the Business Contact details of the "Human Handler" of the AI model responsible for its functioning as part of the licensing contract
3	The AI developer shall document the Training and Testing process adopted for the development of the model.
4	The AI developer shall document a Risk Assessment of the model indicating its susceptibility to third party security compromise and the potential harm to the user or data principals whose personal data may be processed as well as the society at large.
5	The AI developer shall document the Guardrails incorporated in the AI model to mitigate the security risks
6	The AI developer shall document the default configuration of the model.
7	The AI developer shall incorporate a set of comprehensive instructions to the users on any re-configuration or re-training that may be suggested, required or is expected in its normal use
8	The AI developer shall incorporate a set of emergency handling instructions in case the AI has a risk of hallucination or going rogue.
9	The AI developer shall incorporate a "Kill Switch" which is reasonably tamper proof.
10	The Kill Switch shall be configured so as not to be accessible by the Model and shall be controlled in a separate chip or circuit that can be accessed independently with a provision that if the Model tries to access the Kill Switch, the Algorithm should self-destruct.
11	The AI model shall be audited by an independent third-party auditor using an acceptable audit standard.

12	If the AI is classified a "Critical Risk" taking into consideration its autonomy, the type of sensitive data it is expected to process and the automated decision-making capability that could affect the society, a post implementation behaviour monitoring shall be made available at the choice of the deployer.
13	The AI developer shall document the use of AI agents as part of its work force and its likely impact on the AI algorithm/Model developed

For any clarifications, contact Naavi founder of www.naavi.org and Chairman of Foundation of Data Protection professionals in India (www.fdppi.in)

This is released in public interest and is requested to be used responsibly. Suggestions for modifications are welcome. FDPPI will be open to improvements and a special committee for the purpose would be available at FDPPI.

Comments can be sent to dgpsi@naavi.org .