ISO 9001-2015

# Andhra Chamber of Commerce

(INCORPORATED UNDER SECTION 8 OF THE COMPANIES ACT)

"Velagapudi Ramakrishna Bldg.", 23, Third Cross Street, West C.I.T. Nagar, Nandanam, P.B.No.3368, Chennai-600 035
Phone: 044-24315277 / 78 / 79, Email: andhrachamber1@gmail.com / acc@andhrachamber.com
Web: www.andhrachamber.com

To

5.3.2025

Hon' Shri Ashwini Vaishnaw
Ministry of Electronics and Information Technology,
Government of India,
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi – 110003

Respected Sir,

**Sub: Representation to the Ministry of Electronics and Information Technology , Government of India**

Andhra Chamber of Commerce places on record its deep and sincere appreciation of the initiative of the Ministry of Electronics and Information Technology (MeitY) active in regulating the processing of digital personal data, respecting individuals' right to protect their data while at the same time recognising the necessity of processing and using such data for lawful purposes.

The Digital Personal Data Protection Act, 2023 (Act) received the assent of the Hon'ble President on 11th August 2023 and a Draft of the Rules as envisaged under different sections of the Act have been made. The Rules provides for the necessary details and implementation framework of the Act. MeitY has called for feedback on the Draft of the Rules with ground-level concerns and suggestions for modifications and adaptation.

Andhra Chamber of Commerce submits the following opinions for consideration by MeitY .

Dr V L Indira Dutt
President

**SECUNDERABAD OFFICE:** "T.G. Venkatesh Bhavan", R-602 & 603, Chenoy Trade Centre, VI Floor, 116, Park Lane, P.B.No.1716, Secunderabad-500 003 (T.S.)
PHONE: 040-27840844, Email: andhrachamber@gmail.com

**VISAKHAPATNAM OFFICE:** D.No. 1E, 1st Floor, Sai Sadan Apartments, Near Diamond Park, Dwaraka Nagar, 3rd Lane, Visakhapatnam - 530016 (A.P).
PHONE: 0891-2792220, Fax: 0891-2792221, Email: andhrachamberofcommercevizag@gmail.com

**VIJAYAWADA OFFICE:** Siddhartha Hotel Management College Premises, Pinnameneni Poly Clinic Road, Technical Nagar, Vijayawada - 520 010 (A.P).
PHONE : 0866-2472500, Email: andhrachambervijayawada@gmail.com

**NELLORE OFFICE:** No. 24-2/395, Saraswathi Nagar, Magunta Lay-Out, Nellore - 524 003 (A.P). Email: andhrachambernellore@gmail.com

| S No | Title | Description (As per the GN dated Jan 3, 2025) |
|---|---|---|
| 1 | Consent Management | Clear, standalone, and easy-to-understand consent forms. |
| | | Data Principals can withdraw consent as easily as it was given. |
| 2 | Rights of Data Principal | Right to access, correct, erase, and port personal data. |
| | | Right to be informed about data breaches. |
| 3 | Obligations of Data Fiduciaries | Implement strong security measures (e.g., encryption, access control). |
| | | Notify data breaches within 72 hours. |
| 4 | Processing of Children's Data | Mandatory verifiable parental consent. |
| | | Prohibited from tracking or targeted advertising. |
| 6 | Cross-Border Data Transfers | Allowed to whitelisted countries or with adequate safeguards |
| 8 | Significant Data Fiduciaries | Must conduct annual Data Protection Impact |
| | | Assessments (DPIAs). |
| | | Subject to enhanced audits and compliance checks. |
| 7 | Data Retention | Retain personal data only as long as necessary; delete |
| | | when no longer required. |
| 8 | Penalties for Non-Compliance | Fines up to ₹250 crore for serious breaches. |
| 9 | Grievance Redress Mechanism | Data Fiduciaries must appoint Grievance Redress |
| | | Officers and resolve issues within a defined timeframe. |

| Clause Ref | Topic | Observation | Description | Reference & Addl |
|---|---|---|---|---|
| **Rule 3** | **Notices in simple language** | No specific format or structure is prescribed for the notice, leading to possible inconsistencies in its presentation across Data | Rule 3 addresses about notice requirements, but not specified any methods to be followed . It should be in simple language including digital and physical form , to be understood by the Individual, not in a technical language | Refer Rule 3(1) |
| **Rule 4 of 3** | **Consent Mechanism** | The draft rules lack detailed technical and operational standards that Consent Managers must adhere to, leading to potential inconsistencies in implementation. | Consent Managers must demonstrate compliance with technical and organizational standards specified by the Board.<br><br>Also lack of clarity on the timelines<br><br>Need to specify the timeline for DF about withdrawal of consent and period to be specified, i.e. no of days | Rule 4(3) discusses consent management but does not specify any timelines. |
| **Rule 6** | **Standards & Security Measures** | The rule defines certain security measures but does not fully clarify what qualifies as "reasonable," leaving it open to interpretation. | Lack of specific standards<br><br>Encrption Mechansim should be in place and pseudonimation of PII & SPII data<br><br>Technical measures such as encryption, pseudonymization, firewalls, and secure coding practices;<br><br>Organizational measures such as access controls, staff training, and incident response plans<br><br>Physical measures to protect data storage facilities and other relevant infrastructure<br><br>On an yearly basis VAPT asssessment needs to be carried out, for MNC and Corporates atleast once in 3 months. | ISO 27001 Standards |
| **Rule 7** | **Breaches '** | The rule does not specify the exact time within which the Data Fiduciary should become aware of the breach, leaving a potential window for delay in reporting. | Lack of specific timelines. As in case of EU- GDPR, it should be initmated within 72 hours by DF / SDF for the data principals Inline with Global Standards | EU GDPR |
| **Rule 8** | **Data Minimization** | The rule does not clearly define what qualifies as a "specified purpose," leading to inconsistency in data retention policies. | Clearly state that only required data which is necessary for specified purposes should be collected and processed.<br>To ensure compliance with data minimization, reviews need to be considered by DF in coordination with the Internal Stakeholders | Not considered |
| | **Data Retention & Removal** | | Need more information about the retention period , industry specific wise and removal of data from the data repository | Lacks detailed |
| **Rule 9** | **Greivance Mechanism** | The rule does not specify what constitutes sufficient or complete contact information, which may lead to inconsistency in providing details to Data Principals. | No clear picture about how to address the greivances and what counter measures need to be taken by DF like timelines to address the greivances and information should be specific in local language<br><br>Implement Greivances redressal system, define timelines for responding the Greivances | Not considered |
| **Rule 10** | **Children's Data** | While the rule emphasizes obtaining consent from the guardian of a child or a person with disability, it lacks detailed guidelines on how to verify guardianship for all possible scenarios. | Lack specifics on the mechanisms to verify the requirement of verifiable parental consent for processing children's data and there is no specific method need to be followed in the latest notification<br><br>Audits needs to be conducted om a periodical basis by DF, to protect Children's data. | Requires more clarity |

| Clause Ref | Topic | Observation | Description | Reference & Addl |
|---|---|---|---|---|
| Rule 11 | Exemptions, Schedule IV - Part A & B | The rule mentions that the exemption applies if processing is carried out in accordance with the standards specified in the Second Schedule, but these standards are not explicitly | Need detailed information about exemptions, only healthcare and educational institutions are taken into consideration, need a robust framework<br><br>Schedule 9(1) - Verifiable Parental Consent & 9 (3) Tracking and Behavioral Monitoring shall not apply mainly for Healthcare and Educational Institutions | Detailed framework needed , industry wise |
| Rule 12 | Audits and Assessments | The rule does not specify the exact elements or areas to be covered by the DPIA, potentially leading to inconsistent assessments. | Needs to conduct periodic audits DPIA to protect the PII and SPII and maintain the privacy , but frequenct of the audit and it's scope are not clear<br><br>Need to be mandated to conduct third party audit for SDF | Need an elaborate information including guidelines |
| Rule 13 | Rights to Data Principals | The rule mentions the rights of Data Principals without providing detailed descriptions or examples of the specific rights they can exercise under the Act.<br><br>No Specification how grievances should be tracked or the minimum quality standards for such systems. | a. Provides a general framework to handle DP, but lacks a lot of vital information and requires further action<br><br>b. All EU GDPR principles need to be mandated like Right to act, Rights to be forgotten, Rights to eraser etc., | About data principal rights but requires further granularity.. |
| Rule 14 | Cross Border Transfer of Data | The rule specifies that personal data transferred outside India must meet the requirements set by the Central Government but does not clarify what those specific requirements or conditions are, leaving room for uncertainty. | The Draft bill provides Cross Border Transfer of data for specified countries, white listed countries by GOI, but there is no clarity on the data transfer.<br><br>a. How the receipent country is going to protect the PII / SPII<br>b. Is there any data protection mechanism exist.<br>c. Need speicifc standards for the white listed countries incorporating contractual clauses for cross border transfer of Data from GOI on DPDP. | Need more clarity incl rules and regulations with Contractual Obligations |
| Rule 16-21 | | To form a Data Protection Board by the Central Government | Formation of Data Protection Board by GOI , appointment of Chairperson and othe rmembers , Fixing up of remuneration fee etc., Board functions and procedural meeting etc., fixing up of fee associated with filing | Central Government Functions |
| Rule 22 | | Penalties for Non-complaince and breaches happened | Need more clarity about the penalties about non-compliance<br><br>Based on the severity of the breaches happened Penalties should be imposed and slab for penalties, category wise, as indicated in DPDP Act 2023, needs to be revisted for the benefit of Startup's / MSME's / Corporates etc., .<br><br>The Act specifies penalties based on the nature and severity of violations. These may include fines of up to ₹250 crore for significant breaches.<br><br>Also Penalties should be in line with global standards like EU GDPR, CCPA etc.,<br><br>In EU GDPR, penalities are based on the turnover between 2% to 4% or the amount fixed by EU., whichever is on the higher side. | Lacks Clarity, need more clarity<br><br>DPB can impose penalties , based on the nature of the breaches happened |

| Sl No | Topic | Description | Reference & Addl Information |
|---|---|---|---|
| 1 | **Grievance Redressal Mechanism** | Grievance redress mechanism lacks detail.<br>- Timelines needs to be defined to addres grievances, say 15 days.<br>- Needs to ensure the availability of grievance mechanisms in local languages. | Rule 9 addressed grievance redress but needs more operational information in detail. |
| 2 | **Latest Emerging Technolgies on AI & ML** | AI Driven decision making mechanism<br><br>Need to mandate transparency in automated decision-making processes; Data fiduciaries to provide a viable explanations for decisions impacting data principals. | Not taken into consideration |
| 4 | **Reporting Structure** | Reporting requirements for DF incldluing SDF are missing.<br><br>Need to mandate annual transparency reports detailing data processing activities, compliance measures, no of breaches, assessment reports etc., . | Not taken into consideration |
| 5 | **Data Retention and Secure Disposal** | Data Handling inlcuding breaches<br><br>Need to define mandatory data retention periods category wise, applicable for each domain industries. Also to ensure that secure disposal protocols are in place mainly for data erasure . | Lack of clarity on rule 8 about data retention |
| 6 | **Data Minimization** | Clearly state that only required data which is necessary for specified purposes should be collected and processed. To ensure compliance with data minimization, reviews need to be considered by DF in coordination with the Internal Stakeholders | Not considered |
| 7 | **Storage of PII / SPII including localized storage** | Critical personal data should be stored within India to enhance data sovereignty.<br><br>Only after ensuring equivalent security measures in the respective countries, cross-border transfers of data, both PII & SPII, to be transferred / allowed. | Rule 14 - Cross-border Transfer of Data<br><br>Lack of clarity on localized storage requirements for PII / SPII critical data. |
| 8 | **Standards and Guidelines** | Need tp ensure that the Data Protection Board updates standards on technical , organzational, physical security on a regular basis, in line with Global Standards and development Including cybersecurity threats. | Not considered |