CHAPTER [7]: Network Data Governance

Version History

Version	Date	Description
0.3	3rd October 2022	Released to NPs
1.0	22nd October 2022	- Added a definition of Personal Data - Removed consent requirement for utilising anonymised, aggregated data - Aligned requirements for notifying data subjects of breaches of data pertaining to them with existing standards - Added obligation on ONDC to store any Personal Data collected from NPs in a secure manner as per the law

7.1. Personal data with Network Participants

7.1.1. The Network Participants shall adhere to all Applicable Laws governing privacy and data, and hereby agree to utilise any Personal Data about a natural person, living or deceased, which is received, provided or in the possession of the Network Participant only as consented to by such natural person, or as per Applicable Laws.

7.1.2. The Network Participants shall be responsible for the compliance related to all Personal Data in their possession, for processing, transmitting, storing, using, disclosing, sharing, dealing, handling or transferring Personal Data relating to natural persons on the ONDC Network.

7.1.3. If the Network Participant engages any service provider, including but not limited to Technology Service Providers, for offering its services or products on the ONDC Network, it shall ensure that such service provider also complies with this clause 7.1.
For clarity, the term "service provider" in this clause shall not include any other Network Participant that is a counterparty in a transaction on the ONDC Network.

7.1.4. The Network Participant shall ensure that it obtains the necessary consents under the Applicable Laws for processing, transmitting, storing, using, disclosing, sharing, dealing, handling or transferring Personal Data relating to natural persons on the ONDC Network. The consent must be explicit, and in accordance with Applicable Laws, and the purpose for which the consent is being obtained must be clearly communicated to the natural person before taking the consent.
To clarify, Network Participants shall be responsible for collecting consent from their respective End User. The Buyer App shall be responsible for taking consent from the Buyer, and the Seller App shall be responsible for taking consent from the Seller. The Network Participant collecting consent from their End User shall be responsible for conveying it to the other Network Participants, as required.

7.1.5. The Network Participant shall publish a privacy policy providing notice with respect to its handling or dealing with Personal Data in accordance with the Applicable Laws.

7.1.6. The Network Participant shall ensure that any entity processing data on its behalf also complies with Applicable Laws in relation to such processing.

7.1.7. The Network Participant will put in place adequate security measures and frameworks, such as encryption, authentication and authorisation, anonymisation, masking, network-level security apparatus etc, to protect Personal Data, whether the data is at rest or in transit.

7.1.8. Should a Network Participant become aware of any unauthorised access of any Personal Data held by it, it will notify the person, to whom the Personal Data pertains, without undue delay as prescribed by the Applicable Laws.

7.2. Personal Data collected or received by ONDC

7.2.1. ONDC may, over the course of its operations, including in relation to grievance redress, operating the ONDC Network or for ensuring compliance with the ONDC Network Policy, receive or collect Personal Data about a natural person, living or deceased. ONDC may also collect Personal Data from Network Participants where the Network Participants themselves share Personal Data while onboarding onto the ONDC Network. In case the Personal Data is received from the Network Participants (for purposes other than the onboarding of such Network Participants), the Network Participants would be required to obtain consent from the natural person on behalf of ONDC for the purposes of using, storage, sharing, disclosure, transfer, dealing, handling or processing of the Personal Data of the natural person under the Applicable Laws. All data collectively stored, transferred or received by ONDC from the Network Participant will be securely stored by ONDC as per Applicable Laws.

7.2.2. In case, ONDC directly collects Personal Data, it shall be responsible for obtaining consent for the purposes of using, storing, sharing, disclosure, transfer, dealing, handling and processing of the personal data of the relevant individual under the Applicable Laws. The consent must be explicit, and the purpose for which the consent is being obtained must be clearly communicated to the natural person before taking the consent.

7.2.3. ONDC shall publish a privacy policy providing notice with respect to its handling, transferring or dealing with Personal Data.

7.2.4. ONDC shall not be responsible for ensuring the accuracy of Personal Data received from Network Participants. The Network Participant shall be responsible for ensuring the accuracy of data and taking necessary consents under the Applicable Laws for sharing such Personal Data.

7.2.5. ONDC may use anonymised and aggregated data as per the ONDC Network Policy.

7.2.6. ONDC will put in place adequate security measures and framework, such as encryption, authentication and authorisation, anonymisation, masking, network-level security apparatus etc, to protect Personal Data, whether at rest or in transit.

Open Network for Digital Commerce

Summary of Consultations

ONDC sought inputs from the various Network Participants, both onboarded and prospective, and other stakeholders on Chapter 7 Network Data Governance (v0.3). Summarised below are the feedback/queries received from Stakeholders and ONDC's responses to them.

1. **Scope of personal data**

Clause 7.1.1 casts an obligation on all Network Participants to comply with laws related to privacy and data, and requires them to only utilise the data as per the person's consent or applicable law.

Stakeholder Inputs

Stakeholders have raised two queries:

(a) What is included under the definition of personal data?
(b) What about consent for use of business data such as seller catalogues?

ONDC's Response

ONDC clarifies that what constitutes Personal Data will be determined by law, however depending on the requirements of the ONDC Network, ONDC may designate other personally identifiable information as Personal Data, that would fall under the ambit of this chapter of the ONDC Network Policy. It is further clarified that for the time-being, the Applicable Law from which the definition is drawn is the Information Technology Act, 2000, and the rules made thereunder; specifically, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

ONDC further clarifies that this chapter is only intended to cover data pertaining to natural persons. Business data falls under the purview of the confidentiality provisions of the chapter on code of conduct and data-handling related provisions of other chapters. As an example, Buyer Apps are allowed to cache seller catalogues, but they have to respect the TTLs specified by the Sellers / Seller Apps.

2. **Obtaining and managing consent**

Clause 7.1.4 requires all Network Participants to take explicit consent from the data subject and utilise the data only as per the person's consent.

Stakeholder Inputs

Stakeholders gave the following feedback:

(a) How will a Buyer App take consent from the Seller and the Seller App from the Buyer since they do not have any contractual relationship?
(b) If any of the data are anonymised the consent requirement should not apply
(c) How should this clause be interpreted by Logistics Service Providers who do not directly receive data from any End User or natural person?
(d) When would ONDC require personal data from the NPs?

ONDC's Response

ONDC clarifies that the Buyer App would be responsible to take consent from the Buyer and the Seller App from the Seller, and convey the same to the other Network Participants involved in the transaction. An explanation to this effect has been added.

On the point of consent for utilisation of anonymised data, ONDC agrees with the contention of the stakeholders, and the clause has been suitably amended.

On the question of how the consent requirement applies to Logistics Services Providers (LSPs), since LSPs do not directly collect data from End Users who are natural persons, they are not responsible for obtaining consent. They do however, have to respect the terms of the consent as reported by the Network Participant from whom they receive Personal Data.

On what data ONDC would require from Network Participants, ONDC may ask for data in the course of fact-finding/investigation in relation to a complaint against a Network Participant. ONDC does not and will not ask for Personal Data in any other scenario, except when required to comply with the law or an order from a competent authority.

3. **Informing data subjects about data breaches**

Clause 7.1.8 requires all Network Participants to inform persons, whose data may have been compromised, of such a breach within 72 hours of discovery of the breach.

Stakeholder Inputs

Stakeholders have contended that existing laws in India do not require a time-bound breach notification to be sent to the data subject. They only require the appropriate government/regulatory authority to be notified. Consequently, stakeholders have suggested that this requirement be dropped, or be amended to simply require reporting as per Applicable Laws. Stakeholders have further pointed out that the Personal Data Protection Bill is likely to be reintroduced in the Indian Parliament in the near future, and it is expected to prescribe how Personal Data breaches have to be treated.

ONDC's Response

ONDC recognises that neither the existing laws in India nor laws in other jurisdictions such as the US and EU explicitly lay down a timeline for reporting breaches to data subjects. However, Article 34 of the GDPR does specify that if a data breach has the potential to cause harm to a data subject, the data controller must report the breach to the data subject without undue delay.[1] ONDC has amended the provision to strike a balance between easing the compliance burden as requested by the stakeholders and protecting data subjects.

4. **Scope of ONDC's collection of personal data from Network Participants**

Clause 7.2.1 places an obligation on Network Participants to obtain consent from data subjects to share personal data with ONDC when it is necessitated, for example, for ensuring compliance with the ONDC Network Policy or for grievance redress.

[1] See Article 34 of the GDPR (https://gdpr-info.eu/art-34-gdpr/)

Stakeholder Inputs

Stakeholders requested that the elements of such data be described so that they can take consent from their respective End Users accordingly.

ONDC's Response

ONDC clarifies that the exact fields that may be required may change from case to case. Therefore, ONDC has given the purposes for which it may ask for personal data. The actual fields that may be required cannot be reasonably specified a priori.

5. **ONDC's Privacy Policy**

Clause 7.2.3 places an obligation on ONDC to publish a privacy policy.

Stakeholder Inputs

Stakeholders requested that the scope of the privacy policy should include data transferred to third-parties for the scoring and badging.

ONDC's Response

ONDC acknowledges the suggestion. This proposal will be taken up for consideration when ONDC formulates its privacy policy.

6. **Responsibility of ensuring accuracy of personal data**

Clause 7.2.4 states that ONDC shall not be liable for any inaccuracies in the Personal Data received from Network Participants and that the Network Participant shall be responsible for ensuring the accuracy of data and taking necessary consents under the Applicable Laws for sharing such Personal Data.

Stakeholder Inputs

Stakeholders contended that Buyer Apps cannot guarantee the accuracy of the data, since they are not performing a KYC of their users..

ONDC's Response

ONDC clarifies that this provision is merely intended to exclude ONDC from any liability arising out of inaccuracies in Personal Data provided by the Network Participants. Further, the clause is intended to clarify that the Network Participant has to put in checks to ensure accuracy to the extent they can, and design their terms and conditions for users accordingly.