ENERGY: Now AND Next

DATA PROTECTION POLICY

Issued on 15th February 2024

Version 1

Data Protection Policy

Scope

The purpose of this policy is to ensure compliance with the Data Protection Act (DPA) 2018 which govern any processing of information about living individuals and the rights those individuals have relating to this information. This legislation covers all personal information held in both electronic form and manual form.

This policy applies to all parts of ONGC and to all personal data held and processed by the organization. This includes data held in any system or format, whether electronic or hard copy.

Adherence to this policy is mandatory for all employees of ONGC whether permanent, fixed term or temporary, reviewers, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with ONGC. Non- compliance could lead to disciplinary action.

Data Protection Principles

The data protection principles state that personal data should be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes forwhich they are processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be takento ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Data processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

ONGC's policy ensures processing of all personal data should be safe, secure, ethical and transparent and we have procedures in place to enable data subjects to exercise their rights:

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure and training for compliance with the data protection laws
- We record consent at the time it is obtained and evidence such consent where requested
- We have a robust and documented Complaints Procedure and Data Incident Reporting policies for identifying, investigating, reviewing and reporting any breaches or complaints about data protection
- We store and destroy all personal information in accordance with our Information Retention policy
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- We maintain records of processing activities.

We conduct audits to identify, categorize and record all personal data that is processed outside of ONGC, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing may include (but is not limited to):

- IT Systems and Services
- Legal Services
- Payroll
- Insurance
- Financial sustainability, management and governance checks
- Direct Marketing/Mailing Services.

We have due diligence procedures and measures in place to review, assess and background check all processors prior to forming a business relationship.

Data Governance

Employee Personal Data

We do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with appropriate information about how we process their data.

Data Storage

Information and records relating to data subjects will be stored securely and will only be accessible to authorized employees. Information will be stored for only as long as it is neededor in accordance with the required statute and will be disposed of appropriately.

Data Retention

Data pertaining to exit employees, trainers, learners, clients, vendors, consultants and stakeholders will be retained for a period of two years following their departure from the company. This includes but is not limited to personal information, employment records, and relevant communications. Such data will be securely stored in compliance with applicable data protection regulations. After the retention period, all retained data will be promptly and securely disposed of in accordance with the company's data retention and destruction procedures.

Access to retained data will be restricted to authorized personnel solely for legitimate business purposes or legal requirements.

Data Accuracy

ONGC takes reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

Training

ONGC is committed to a staff awareness programme ensuring that new and existing employees, trainers, learners, clients, vendors, consultants and stakeholders are trained, assessed and supported in a variety of ways to discharge their data protection responsibilities in a variety of ways, including Online and virtual induction including a test at the end of each module

- Online induction training with a test at the end of each module
- Virtual training which focuses on ONGC policies and procedures
- Annual refresher training covering data protection, records management, information security and cyber security that is delivered in group sessions either face to face or virtually.

- Regular awareness updates and alerts to any information security risks
- 1:1 support session as and when necessary
- Access to data protection and information security policies, procedures, checklists and supporting documents.

Data Storage and Deactivation for Exit Employees

- Upon separation from the company, all exit employees, trainers, learners, clients, vendors, consultants and stakeholders must adhere to the data storage and deactivation protocol.
- Exit employees are required to securely transfer all company-related data from personal devices to designated storage platforms.
- Personal cloud storage accounts used for work-related data must be promptly deactivated.
- Any physical storage devices containing company information must be returned to the IT department for data wiping or disposal.
- Email accounts and access credentials must be surrendered and will be deactivated to prevent unauthorized access.
- Collaboration tools and shared drives must be cleared of any personal or sensitive information before departure.
- Exit employees must cooperate with IT personnel to ensure proper data removal from all devices and platforms.
- Failure to comply with data storage and deactivation procedures may result in disciplinary action or legal consequences.
- The company reserves the right to monitor and audit compliance with this policy to safeguard sensitive information.
- By acknowledging this policy, exit employees agree to abide by its terms and protect the integrity and confidentiality of company data even after departure.

Penalties for Non-Compliance

ONGC understands its obligations and responsibilities under the data protection laws and recognizes the severity of breaching any of these.

It is the responsibility of all, employees, trainers, learners, clients, vendors, consultants and stakeholders to:

- Ensure that they collect, store and process personal data in accordance with

"data protection laws" and comply with ONGC's Data Protection Policy.

- Only use personal data for the purpose of their contracted duties.
- Store contacts in approved and managed systems and not held in duplicate copies elsewhere.
- Not attempt to gain access to information that it is not necessary for them to hold, know or process.
- Ensure that any personal data obtained is accurate and relevant to the purpose for which it is required.

Escalation Matrix:

In the event of non-compliance or disputes regarding data storage and deactivation, relevant stakeholder should follow the established escalation matrix as given below

ESCALATION MATRIX - Triggers on		
First Level (SPOC)	Second Level (SPOC)	Third Level (SPOC)
Name – Mr JVH Prasad	Name – Mr Antonio JL Gomes	Name – Mr Sanjeev Singhal
Designation – GM - Production	Designation – GM – Production	Designation – Executive Director
Contact No +91 9491069164	Contact No +91 9422460259	Contact No +91 9405305850
Email - prasad_jvh@ongc.co.in	Email - gomes_aj@ongc.co.in	Email - singhal_sanjeev@ongc.co.in

Policy Review

This policy will be updated on a yearly basis or as necessary to reflect best practice, relevant case law, and to ensure compliance with any changes or amendments to Data Protection legislation.

ONGC IPSHEM conducts an annual review of this policy and associated documentation. Updates and communications regarding reviews will be shared with relevant employers, along with any specific outcomes resulting from the reviews, as appropriate.

Date: 15.02.2024

Place: Goa

Executive Director - HOI

ONGC IPSHEM, Goa

संजीव सिंघल
कार्यकारी निदेशक – संस्थान प्रमुख
इप्शेम, ओ. एन. जी. सी., बेतुल, गोवा
Sanjeev Singhal
Executive Director - Head of Institute
IPSHEM, ONGC, Betul, Goa