INDO COUNT INDUSTRIES LIMITED

DATA PRIVACY POLICY

Version No.: 1.1
Version Date: 25-12-2023
Approved by: Board of Directors

A. OBJECTIVE

Indo Count Industries Limited ('ICIL' or 'the Company') is committed to respect privacy of every person, including employees of the Company, business partners as well as vendors, dealers, customers, and other stakeholders who share their Sensitive Personal Data or Information with the Company. This privacy policy ('Policy') is applicable to all stakeholders who disclose Sensitive Personal Data or Information to the Company ('stakeholders') for fulfilling lawful business requirements of the Company.

The objective of this Policy is to give stakeholders an understanding on how the Company intends to collect, receive, possess, store, transfer, handle, deal with and use the Sensitive Personal Data or Information ('SPDI') provided. All data collected will be treated as per the regulations outlined in the Digital Personal Data Protection (DPDP) Act, 2023.

B. SCOPE OF APPLICABILITY

This policy applies to all stakeholder SPDI that the Company collects and holds in the course of conducting its business.

C. Data Classification

a. **Biometric data:** means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioral characteristics of a data principal, which allow or confirm the unique identification of that natural person.
b. **Financial data**: means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a bank/financial institution and a data principal including financial status, income, wealth status and credit history.
c. **Genetic data:** means personal data relating to the inherited or acquired genetic characteristics of a natural person which provides unique information about the behavioral characteristics, physiology or the health of that natural person and which results, in particular, from an analysis of a biological sample from the natural person in question.
d. **Personal Data:** Data from which an individual can be identified like name, address, sex, religion, caste, etc.
e. **Sensitive Personal Data or Information or Information (SPDI):** Types of personal data such as financial, health, blood group, sexual orientation, biometric, genetic, transgender status, belief etc.

The Company may collect the following types of Sensitive Personal Data or Information or Information, including but not limited to:

a. Name, address, contact numbers, email ID, details of past employment (in the case of employees, wherever relevant);
b. Family details, their addresses, contact numbers, email ID, relationships, family history etc.
c. Financial details such as bank account, pan card, salary slips, provident fund details, Income Tax Returns, other Tax Returns.
d. Blood group, medical history, physiological and mental health condition, sexual orientation etc.
e. Biometric information.

D. The Digital Personal Data Protection (DPDP) Act, 2023

The Indian Parliament passed the Digital Personal Data Protection (DPDP) Act, 2023 in August 2023. The DPDP Act aims to prevent online platforms from misusing personal data. It is the first cross-sectoral law in India to protect personal data.

The DPDP Act gives individuals the right to:

a. Access their processed data.
b. Correct their data.
c. Erase their data.
d. Have their grievances redressed.
e. Nominate someone to exercise their rights if they become incapacitated or die.

The DPDP Act also requires data fiduciaries to:

a. Delete data when a data principal withdraws consent.
b. Share information about processors they have engaged with if requested by a data subject.
c. Store at least one copy of personal data in India

The DPDP Act includes a penalty of up to Rs. 250 crore for companies or entities that misuse or fail to protect digital data.

E. Data Gathering

The Company may collect, use, receive, possess, store, disclose, process, and transfer the Sensitive Personal Data or Information for various purposes, including but not limited, to the following:

- To enable the functioning of the Company's business.
- In connection with a variety of purposes relating to employment or engagement of employees or training including but not limited to general HR administration; organization planning and management.
- Compliance with the company's policies, code of conduct, and internal policies and regulations.
- Business mergers and acquisitions; business transfers, business restructuring, etc.
- Legal & judicial proceedings, governmental and regulatory compliance.
- Tax administration and compliance.
- Overseas affiliates' compliance with foreign laws and cooperation with overseas regulators.
- To transfer to IT services providers/Software developers.
- To administer or otherwise carry out obligations with any agreement which has been executed by the Information Providers with the Company.
- To investigate, prevent, or act regarding illegal activities, suspected fraud, violations of the law, or as otherwise required by law.

The Information Providers consent that the collection, usage, storage, disclosure, processing, and transfer of any Sensitive Personal Information or any other information as disclosed under this Policy shall not cause any loss or wrongful gain to the Information Providers if the same is used for the above-mentioned lawful purposes.

F. Collection of Information

We may collect information that you share with us through your use of our website, for example by: - E-mailing or writing to us using the contact details posted on our website; or - Submitting other inquiries.

G. Our Use of Your Information

Our primary goal in collecting personally identifiable information is to provide you with a smooth, efficient, and customized experience. We may use the information we collect from you when you register, make a purchase, sign up for our newsletter, respond to a survey or marketing communication, surf the website, or use certain other site features.

H. Uses of Cookies

The Website may use "cookies" (information stored on Your computer/Your Computer Resources which include mobile phones and APPs) by your browser at our request). Cookies may be used to identify users and qualify as personal data. To comply with the regulations governing cookies under the privacy law ICIL must:

- Receive data subject to consent before ICIL uses any cookies except strictly necessary cookies.
- Provide accurate and specific information about the data each cookie tracks and its purpose in plain language before consent is received.
- Document and store consent received from the data principal (A living individual to whom personal data relates).
- Allow data principals to access ICIL services even if they refuse to allow the use of certain cookies.
- Provide a convenient process for data principal to withdraw their consent.

All information collected by these third party cookies is aggregated and anonymous. By using the Company's website, the user agrees that these types of cookies can be placed on his/ her device. User is free to disable/ delete these cookies by changing his/ her device / browser settings. The ICIL is not responsible for cookies placed in the device of user/s by any other website and information collected thereto

I. Data Transferring or sharing:

- The Information providers understand and consent that the Company may need to share the Sensitive Personal Data or Information with its affiliates, group companies, business associates and/ or third parties within and outside India, in connection with the lawful purposes, as mentioned above.
- The Information Providers authorize the Company to exchange, disclose, transfer, share, and part with the Sensitive Personal Data or Information and/or any information provided, within or outside India for the above purposes.

J. Confidentiality of the data processing

Only authorized employees or persons authorized by the Company process personal data. It is forbidden for employees to use personal data for their own benefit/purpose, to transmit these to unauthorized persons, or to make these accessible in any other manner.

K. Reasonable Security Practices and Procedures

- The Company has adopted reasonable security practices and procedures to ensure that the Sensitive Personal Data or Information is collected and preserved securely. Suitable measures are taken to protect the data against accidental or unauthorized destruction or against loss.
- In case the Information Providers wish to know more details about the adopted reasonable security practices and procedures, they may contact the Data Protection Representative of the Company for the same.

- The Company will endeavor to take all reasonable and appropriate steps to keep secure any information and prevent its unauthorized access and transfer, the information providers agree and acknowledge that the Company cannot provide any absolute assurance regarding the security of the Sensitive Personal Data or Information. To the maximum extent permissible under applicable laws, the Company disclaims any liability for any breach of security or loss or disclosure of information with Personal Information.

If the Information Provider needs to access update or correct the Sensitive Personal Data or Information, he/she may contact the Data Protection Representative of the Company for the same.

L. General Staff Guidelines:

The only people able to access data covered by this policy should be those who need it for their work. Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

ICIL will provide training to all employees to help them understand their responsibilities when handling data.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Employees must obtain their Head of Department (HOD) approval and fill up duly signed "Data Copying or Data Transfer Request Form" before sending, transferring, mailing, or uploading of data to third party, customers working with ICIL.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

M. Data Retention & Storage

1. Data Storage:

- These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data controller. When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people can see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

2. Data Retention:

It is the Company's policy to retain Sensitive Personal Data or Information of the Information Providers only for as long as the Company believes it to be necessary for the purpose for which such Sensitive Personal Data or Information was collected, subject to any legal requirements for the information to be retained for a longer period, if any.

N. Data Use:

Personal data is of no value to ICIL unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

O. Lawful Processing of Data:

Consent: The data subject has given their unambiguous consent for the processing of their data.

Contract: The processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject before entering a contract.

Legal obligation: The processing is necessary for compliance with a legal obligation to which the data controller is subject.

Vital interests: The processing is necessary to protect the vital interests of the data subject or another individual.

Public interest: The processing is necessary for the performance of a task carried out in the public interest.

P. Compliance of Policy

- Compliance with this Policy is essential to ensure that appropriate controls are in place.
- Any Individual Employee or Individuals Working for ICIL found to have intentionally violated this Policy may be subject to suitable action including disciplinary action, up to and including termination of employment/ contract under the Digital Personal Data Protection (DPDP) Act, 2023.

Q. POLICY AMENDMENT

The Company reserves the right to revise and update this Policy at any time and any such change will be communicated to all stakeholders through appropriate means.

R. COMPLAINTS

Any grievances or complaints with respect to the data privacy of stakeholders may be addressed to the IT Head of the Company through email at helpdesk@indocount.com. The Company is committed to ensuring a fair and rapid resolution of any complaint or dispute that falls under the ambit of this Policy.