UFLEX LTD.

Privacy Policy

1. Purpose and Scope

We, UFLEX LTD. ("the Company"), respect the privacy of individuals and have implemented reasonable security practices and procedures that are commensurate with the information assets being protected and with the nature of our business.

This privacy policy ("Policy") aims to set out the process and the framework within which the Company collects, receives, stores, deals or handles Personal Information, including Sensitive Personal Data or Information. The Policy covers all the Stakeholders of the Company.

In this Policy, unless the context otherwise requires:

i. 'Personal Information' means any information that relates to a natural person which, either directly or indirectly, in combination with other information available or likely to be available with the Company, is capable of identifying such person.

ii. 'Sensitive Personal Data or Information of a person means such Personal Information which consists of information relating to:

- Password.
- Financial information such as bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health conditions;
- Sexual orientation;
- Medical records and history;
- Biometric information;
- Any detail relating to the above clauses as provided to the Company for providing service; and
- Any of the information received under any of the above Clauses by the Company for processing, stored, or processed under lawful contract or otherwise:

  Provided that any information that is freely available or accessible in the public domain or furnished under the Right to Information Act 2005 or any other law for the time being in force shall not be regarded as Sensitive Personal Data or Information.

iii. The words and expressions used in this Policy but not defined herein but defined in the Information Technology Act 2000 ("IT Act") or the Information Technology (Reasonable

Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("IT Rules") shall have the meanings assigned to them thereunder.

2. Collection of Personal Information

The Company collects Personal Information (which may include Sensitive Personal Data or Information) that is voluntarily provided to it for its business and through responses to job postings, queries, complaints, feedback, etc.

Personal Information: To get access to the Company's website, the user does not need to disclose any personal information. Examples of personal information include name, title, company, address, phone number, email address, details of government identity numbers, and other applicable data. If the user decides to send an email to the Company, just the user's email address, name, and contact number, which are mainly necessary for communication purposes, will be recorded. It will not be added to the Company's mailing list and will only be used for the purpose requested by the user. Except as required by law, the user's email address and other information will never be used for any other reason and will never be made public.

Non-Personal Information: The Company uses this information with the objective of providing a better service experience. Information regarding the number of users linking to the Company's website from a third-party website may occasionally be provided to the owners or operators of such third-party websites, which allow for the creation of links to the website of the Company. This information does not reveal any information related to the user's identification.

By using the Company's website, the user shall agree to the terms of this Privacy Policy. However, if the user does not want UFlex to use, process, or transfer his/her information in any way, then the individual would have the option to refrain from sharing it.

Information collected by the Company during the onboarding of an employee, agreement with a supplier or vendor, or with any other stakeholder while providing services or conducting any business activity, would be secured through stringent data protection and privacy procedures. The Company would ensure to limit access of individuals regarding confidential data and would not make it public.

The Company may store some of the cookies on the user's computer while they visit the website of the Company.

3. Use and Processing of Personal Information (including Sensitive Personal Data or Information)

The Personal Information (including Sensitive Personal Data or Information) collected by the Company may be used for various legitimate business and/ or regulatory purposes.

4. Disclosure and transfer of your Sensitive Personal Data or Information

a. The Company may need to disclose/ transfer Sensitive Personal Data or Information to its service providers or business partners, during the normal course of business, as required to perform the services of the Company. Some of the third parties to which Sensitive Personal Data or Information may be disclosed/ transferred are:

i. Service providers appointed by the Company to carry out services on the Company's behalf under contract.

ii. Company's affiliates in India who may use and disclose such information for the same purposes as the Company.

b. The Company may disclose Sensitive Personal Data or Information

i) to protect and defend the rights or property of the Company.

ii) to fight fraud;

iii) to enforce the Company's policies; or

iv) when the Company, in its sole discretion, deems it necessary to protect its rights or the rights of others. The Company may disclose Sensitive Personal Data or Information if otherwise required by an order under any law for the time being in force including in response to inquiries by government agencies for verification of identity, or for prevention, detection, and investigation including cyber incidents, prosecution, and punishment of offenses.

c. The Company may also disclose or transfer the Sensitive Personal Data or Information, to another third party as a part of reorganization or a sale of the assets or business of the Company.

Any third party to which the Company transfers or sells its assets will have the right to continue to use such Sensitive Personal Data or Information.

d. Company uses its best efforts to ensure that third parties, as stated above, who have access to personal sensitive data will store such information with complete care and confidentiality as if it is their own personal information and treat this information only according to applicable laws.

5. Information provider's rights about their Sensitive Personal Data or Information collected by the Company

a. All Sensitive Personal Data or Information provided to the Company by an information provider is voluntarily provided by such information provided.

b. The information provider may write to the Grievance Officer, whose details are provided in Clause 7 below, to access, review, modify or correct his/her Sensitive Personal Data or

Information. However, the Company is not responsible for the authenticity of the Sensitive Personal Data or Information provided by the information provider.

c. The information provider shall, at any time while availing the services or otherwise; also have the option to withdraw his/ her consent given about his/ her Sensitive Personal Data or Information. However, please note that withdrawal of consent will not be retrospective and shall be applied prospectively. Such withdrawal of the consent shall be sent in writing to the Company at grievance@uflexltd.com. In case the information provider does not provide his/ her information or consent for the usage of Sensitive Personal Data or Information or subsequently withdraws his/ her consent for the usage of the Sensitive Personal Data or Information so collected, the Company reserves the right to discontinue the services for which the said information was sought.

6. Cyber Security Practices and Procedures

The Company has implemented reasonable security practices and procedures (including appropriate managerial, technical, operational, and physical security control measures) to ensure that the Personal Information and Sensitive Personal Data or Information are collected and preserved securely.

To ensure that user information and data is well protected the company follows a comprehensive cyber security practice to prevent any data leakages. Some of the key initiatives taken to protect people and business critical data from getting hacked by cyber criminals is as under : -

- Use of Firewalls,SSL,VPN to regulate external and internal user traffic.
- Use of standard Antiviruses.
- To protect critical servers holding business critical information, company has implemented Privileged Access management (PAM) to ensure users have access to only that information and underlying servers which are needed for discharging their normal duties.
- Secure access to application using Zero Trust Architecture and application virtualization.
- Password based access to business-critical data. Password complexity is also maintained as per recommended best practices (Minimum length, Case Sensitive, Alpha-Numeric Combination, Lock-out duration, Expiration Period, periodic review)
- 24*7 monitoring of all critical applications and underlying IT infrastructure.
- Regular updation of system patches.
- Internet usage is strictly regulated as per policy with suspicious sites and other sites violating defined rules of internet policy are banned for access by users.
- Deployments of anti-spam and related technologies for email security.
- Regular briefing to user community regarding best practices to be followed at work to prevent data breaches by cyber criminals.

- Signing of NDA with service providers so that they also adhere to the provisions of various data and privacy policies and maintain the confidentiality of their tasks and the data /applications/infrastructure or any other critical information they have access to.
- To keep abreast of latest happenings in the field of cyber security, company has a dedicated practice for monitoring cyber security and implementing various available technologies to ensure a safe workplace and build a proper response mechanism to respond to any incident.

Cyber security is an ongoing process with new threads coming at regular time intervals. Company takes all necessary actions which are reasonable and within its reach to implement and ensure confidentiality, integrity and availability of critical business and user data.

7. Grievance Redressal & retention

Any discrepancies and grievances concerning the processing of Personal Information and Sensitive Personal Data or Information shall be immediately informed to the designated Grievance Officer -Mr. Sanjay Kumar Singh; Email: grievance@uflexltd.com; Contact Number: 0120-4002203.

8. Changes to this Policy

The Company reserves the right to revise and update this Policy at its sole discretion based on local government compliances and respective laws. Any such revisions will be effective on and from the date of posting the same on the Intranet/website of the Company and will apply to all information collected both before and following the effective date.

9. STANDARDS REFERRED

The Standards referred to are:

ISO 27001 – Clause 18 Compliance Policy, Applicable Privacy Law by respective Government & GDPR,