LTIMindtree

Global Data Privacy Policy (External)

Version 1.0 | 14 November 2022

Copyright Information

Revision History

Please keep the latest version on top

Ver	Change Description	Sections	Date	Author	Reviewer	Approver
0.1	Initial Document	All	14th November, 2022	Data Privacy Office	Legal	Data Privacy Officer

References

This is a Global Data Privacy Policy, for more information and for more details for each specific activities please refer to the following documents:

No	Document Name	Ver	Location
1.	LTIMindtree General Data Privacy Statement	1.0	https://www.ltimindtree.com/general-privacy-policy/
2.	LTIMindtree Cookie Policy	1.0	https://www.ltimindtree.com/cookie-policy/

Table of Contents

Introduction

Your privacy is important to us. LTIMindtree Limited and its group companies ("LTIMindtree"') is committed to respecting your privacy while using our website (www.LTIMindtree.com). This LTIMindtree Global Data Privacy Policy ("Global Policy") defines the requirements to ensure compliance with the applicable data privacy laws and regulations applicable to LTIMindtree's collection, use, and transmission of Personal Data (the meaning of which is set out below) for information collected by us about you. Protecting the privacy rights of data subjects and safeguarding their Personal Data is now being treated as a basic right of an individual and a legal requirement in many parts of world. LTIMindtree, being a global organization, respects the privacy of data subjects and is committed to complying with the applicable data privacy laws and legislations (including but not limited to EU General Data Protection Regulation 2016/679 (the "GDPR"), the GDPR as saved into UK law (the "UK GDPR") (references in this Policy to GDPR also include UK GDPR) California Consumer Privacy Act, California Privacy Rights Act, The Privacy Act 1988 (Australia) including the Australian Privacy Principles (APP), Data Protection Act 2018 (UK), Information Technology Act 2000 read along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and Personal Data Protection Act 2012 (Singapore), the Federal Law on Protection of Personal data held by Private Parties and its Regulations (Mexico) (the "LFPDPPP, in its Spanish acronym), the Swiss Federal Act on Data Protection 1992 and as of September 1, 2023, the Swiss Federal Act on Data Protection 2020, the Federal Decree-Law No. 45/2021 on the Protection of Personal Data (UAE), the Protection of Personal Information Act 4 of 2013 (South Africa), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and any substantially similar provincial law, Personal Data (Privacy) Ordinance Cap. 486 (Hong Kong), the Personal Information Protection Law ("PIPL") (China), the Privacy Act 1988 (Cth) (Australia) and other applicable privacy laws to the extent that they apply to LTIMindtree's data processing and business operations) (the "Data Privacy Laws").

Policy Statement

This Global Policy is generally designed to explain and set out LTIMindtree's procedures and policies when processing Personal Data, and Personal Information (the meaning of which are set out below) by the organization.

This Global Policy describes how LTIMindtree generally collects, uses and discloses your Personal Data, Personal Information that you provide to us, that LTIMindtree creates, or obtain about you from other sources, as well as the legal bases for processing, and the security measures implemented by LTIMindtree to protect your Personal Data. It also provides you with information about your rights in connection with your Personal Data, and other related details you need to know. LTIMindtree will also inform you of product or service-specific data collection and use which is not reflected in this Policy through supplementary policies or notices provided before the relevant collection of your Personal Data.

Scope

Applicability: The scope of this Global Policy applies to LTIMindtree, its affiliates, business partners, employees, and Third Parties providing services to LTIMindtree (together "LTIMindtree", "We" or "Us"). It covers Processing (including but not limited to collection, storage, usage, transmission and destruction) of Personal Data of LTIMindtree's current and previous employees, prospective candidates, current, prospective and previous customers, current and previous partners/vendors, website visitors, sub-contractors and visitors, (together "you"/ "your") by LTIMindtree during the course of its business activities.Role: LTIMindtree acts as a Data Controller with respect to any Personal Data it holds about you. Please find below its full address and contact information:

LTIMindtree Limited
Gate No. 5, L&T Technology Center,
Saki Vihar Road, Powai,
Mumbai – 400072,

India Phone- +91 22 67766776

Web- www.LTIMindtree.com

LTIMindtree is responsible for ensuring that it uses your Personal Data in compliance with the applicable Data Privacy Laws.

The relevant entities that also act as data controllers are listed in Section 24 of this Policy.

Definitions

The meaning of some of the terms in use in the Policy are explained below:

Term	Description
Personal Data	Means any information relating to an identified or identifiable natural person ("Data Subject"); Any information which constitutes "personal data" or "personal information" of Data Subject under the applicable Data Privacy Laws, including information which can reasonably associate or link to an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This includes the defined term of personal information as defined in Canadian data protection laws. Personal Data includes 'personal information' as defined in the Privacy Act 1988 (Cth) (Australia). With respect to Chinese residents, Personal Data does not include information that has been anonymized. LTIMindtree does not collect Personal Data from Chinese residents that are under the age of 14.
Personal Information (applicable only to California	Information pertaining to residents of California that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, but does not include information that is lawfully made available from federal, state or local government records, nor does it

<table>
<tr><td>residents) (under US laws)</td><td colspan="5">include “de-identified” or “aggregate customer information” as those terms are defined pursuant to the CCPA. LTIMindtree does not collect Personal Information from California residents that are under the age of 16.</td></tr>
<tr><td rowspan="2">Sensitive Personal Data (including specific categories of Personal Data under GDPR)</td><td colspan="5">Pursuant to Article 9(1) GDPR, specific categories of personal data refer to the processing of personal data revealing racial or ethnic origin, or political opinions, or religious or philosophical beliefs, or trade union membership, or the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health or data concerning a natural person's sex life or sexual orientation. Sensitive Personal Data includes ‘sensitive information’ as defined in the Privacy Act 1988 (Cth) (Australia).</td></tr>
<tr><td>For Mexico only: In addition to the preceding, any other categories of personal data that touch the most private areas of the data subject's life, or whose misuse might lead to discriminatio</td><td>For Switzerland only: The definition of “a natural person’s sex life or sexual orientation” also includes the intimate sphere (instead of the sexual life/orientation), social security measures, administrative or criminal proceedings and administrative</td><td>For Chinese residents only: In addition to the preceding, the term also includes other Personal Data of which the leakage or illegal use could easily lead to the violation of the personal</td><td>With respect to California residents, in addition to the preceding, the term also includes government identification numbers, financial numbers or financial account access credentials, precise geolocation, and the</td><td>In Denmark only: Information on social security numbers and criminal offences are not considered as sensitive personal under the GDPR but constitutes its own category of</td></tr>
</table>

	n or involve a serious risk for the data subject are also considered as sensitive data.	or criminal sanctions.	dignity of a natural person or harm to personal or property safety, such as information on biometric identification, financial accounts, personal whereabouts and personal information of minors under the age of 14.	contents of communications to which LTIMindtree is not an intended recipient.	information. Processing of this requires specific legal basis under the Danish data protection act.
zProcess, Processes, Processed or Processing	Means any operation or set of operations which is performed on Personal Data or Personal Information, or on sets of Personal Data or Personal Information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.				
Consent	Means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which the Processing of their Personal Data, Personal Information and/or Sensitive Personal Data via a statement or by a clear affirmative action, signifies agreement to the processing of Personal				

	Data, Personal Information and/or Sensitive Personal Data relating to him or her.
Data Subject	Means to a particular natural person (i.e. an identified or identifiable natural person) to whom Personal Data relates. In case of a minor/ individual with mental disabilities, the data subject would be represented by a legal representative or the holder of parental responsibility (parent/ guardian). For the purpose of clarity of this Policy, "Data Subject" means LTIMindtree current and previous employees, prospective candidates, current, prospective and previous customer personnel, current and previous partner/vendor personnel, website visitors, sub-contractors and visitors. LTIMindtree does not generally process Personal Data/ Personal Information and Sensitive Personal Data from Data Subjects that are under the age of 18 except in specific cases (See. Section 8). For the purpose of CCPA, Data Subject shall include California residents. With respect to Chinese residents, LTIMindtree does not collect Personal Data from Chinese residents that are under the age of 14.
Data Controller	Means the natural or legal person, organization, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by national or applicable laws, the controller or the specific criteria for its nomination may be provided for by national or applicable laws.
Data Processor	Means a natural or legal person, organization public authority, agency or other body which processes Personal Data on behalf of the Data Controller
Third Party	In relation to Personal Data or Personal Information means a natural or legal person, organization, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorised to process personal data;

"Sell," "selling," "sale," or "sold,"	Means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data or Personal Information by the business to another business or a Third Party for monetary or other valuable consideration.
"Share" or "Sharing" (For California residents)	Means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal Information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.
"Protected Health Information" or "PHI" (under US laws)	Means any written, oral, or electronic health information that is created by and/or received from a Covered Entity or a Business Associate of a Covered entity; PHI includes, but is not limited to, any of the following documentation, if the documentation reveals an Individual's identity and the Individual's health status or payment issues: • medical records (such as hospital charts or doctor's notes); • medical bills (such as bills for hospital or doctor's services); • claims data (such as data on claims payments made by the Plans on an Individual's behalf); and • insurance payment information (such as an explanation of benefits).
"Individual" (under US laws)	Means the person who is the subject of the protected health information.
"Covered Entity" (under US laws)	Means any health plan or any healthcare clearinghouse, or any healthcare provider who transmits PHI as per the standards developed by the Department of Health & Human Services ("HHS") in electronic form.

"Business Associate" (under US laws)	Means an entity that performs or assists a Covered Entity with a function or service involving the use or disclosure of PHI. The term Business Associate also applies to subcontractors of a Business Associate entity who perform PHI-related functions.
"Electronic Media"	Means: • electronic storage material on which data is or may be recorded electronically, including devices in computers (e.g., hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or • transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet, intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage me-dia. Certain transmissions, including paper, voice via telephone, and facsimile, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form im-mediately before the transmission.

Please refer to the relevant jurisdiction specific Data Privacy Laws for applicable definitions.

1 What Personal Data/ Personal Information is processed and How we collect your Personal Data/Personal Information

We will collect and process the following Personal Data / Personal Information about you as follows:

Categories of Data Subjects	How We collect your data
Customer Personal Data or Personal Information in Projects including but not limited to identification data (full name, name of your legal representative, signature, ID, national identification ID/number), contact data (address, e-mail, telephone	Directly from you while LTIMindtree providing services to you.

number), tax data (tax domicile, tax registration number); financial data (bank account number, card number); information related to your occupation/business activity	
Business Partner/Vendor Personal Data or Personal Information, including identification data (full name, name of your legal representative, signature, ID, national identification ID/number), contact data (address, e-mail, telephone number), tax data (tax domicile, tax registration number); financial data (bank account number); information related to your occupation/business activity.	Directly from you while LTIMindtree is receiving services from you.
Prospective Candidates, including identification data (name, age, sex, marital status, signature, photo, national identification ID/number); contact information (address, e-mail, telephone number); cv; work history; school history; financial data (socioeconomic study,); information derived from background checks, such as criminal data, and credit history, which may be considered sensitive data (where permitted under local law); information on your personality and skills; personal and work references.	Directly from you in case you have directly applied through the website; From Third Parties or other sources (for example via recruitment agencies or LTIMindtree employee referral but in each case only as far as legally permissible and only as far as is necessary to fulfil the position in question), which may also include public sources such as professional networking platforms or job portals.
Employee Data, including identification data (name, age, sex, marital status, signature, photo, national identification ID/number); contact information (address, e-mail, telephone number); work history; school history; financial data (bank account number,	Directly from you at the time of employment and also during the course of your employment.

salary); information regarding your performance at work; health data, considered sensitive data; other information resulting from the employment relationship.	
Visitor information, including identification data (name, signature, photo, national identification ID/number); and information related to the purpose of your visit.	Directly from you at the time of visiting our premises or by an LTIMindtree employee.
Website Cookies, including information of your device and your navigation habits, some of this information may be considered personal data.	Refer to our Cookie Policy - https://www.ltimindtree.com/cookie-policy/ for information about how we collect information through our website cookies.
Marketing Data, Events and Initiatives	Directly from you when you contact (or you have been contacted) or interact with any LTIMindtree representative, via LTIMindtree website or events or conferences or workshops or Surveys that you attend, by telephone, email, online portal or in person or from professional networking platforms like Linkedin, Twitter.
Prospective Customers and business partners/ vendors, including identification data (full name, name of your legal representative, signature, ID), contact data (address, e-mail, telephone number), tax data (tax domicile, tax registration number); financial data (bank account number); information related to your occupation/business activity.	From other customer/ business partner and vendor referral. Also refer to "Website Data", "Marketing Data, Events and Initiatives".

For California residents only and in addition to the preceding, the categories of sources of Personal Information may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

1 For which and on which legal basis do we process your Personal Data/Personal Information?

Your Personal Data is stored and processed by Us in the following ways and for the following lawful purposes:

- Where you have applied for a role with us, to review and process your job application with Us and (only where legally permissible and where strictly necessary to assess your suitability for the relevant role) to conduct background screening checks on you, including your previous employment, criminal convictions, education, dual employment and other relevant checks (only when permitted or required by the applicable law).
- To carry out activities relating to your employment contract with Us (including, processing your salary, administering benefits, managing and providing training relevant to your role and managing your performance).
- To provide our products and services to you.
- To comply with any legal and regulatory obligations that We have to discharge.
- To establish, exercise or defend our legal rights or for the purpose of legal proceedings.
- Where you are an employee or visitor to our premises, to record and monitor your use of our premises and/or information technology systems in order to maintain its security and protect them against fraud or unauthorised entry (to the extent, and with the safeguards, permitted by the applicable laws).
- for our legitimate business interests, such as operating our website, managing the efficient management and operation of our business, conducting marketing activities designed to improve the products and services We offer to you (subject to obtaining your additional consent as may be required by applicable Data Privacy Laws), targeting advertisements to you on third party platforms and website, and administering the security of our business ("Legitimate Business Interests").When "legitimate business

interests" are not a legal basis for processing under the applicable local law, we will rely on your consent to process your data for these purposes; and

- to prevent and respond to actual or potential fraud or illegal activities.
- Internal Research: We may Process Personal Information for internal research for technological development and demonstration.
- Transactional: We may transfer Personal Information as an asset through a merger, acquisition, bankruptcy or other transaction in which a Third Party assumes control of the business in whole or in part. In such event, the Third Party cannot materially alter how it uses or discloses the acquired Personal Information subject to certain exceptions. For Mexico, your consent is required. By providing us with your personal data and using the website/applying for a vacancy or maintaining a legal relationship with us, you agree to this transfer. However, you may "opt-out", under certain circumstances, according to the procedure included in section 15 "Rights of data subjects".

We Process your Personal Data, Personal Information based on the following legal bases pursuant to applicable Data Protection Laws:

a) Performance of Contract: We process your Personal Data and Personal Information , where necessary in order to take steps at your request prior to entering into a contract or for the performance of a contract with you. For instance, We may process your Personal Data for employment purposes (such as processing your salary, administering benefits) or providing services to our customers which are necessary to execute the contract. If you do not provide Personal Data for processing under this legal basis, We may not be able to perform as per the respective applicable contract.
b) HR Necessity: We may process your Personal Data where necessary for human resources management implemented in accordance with the labour rules and LTIMindtree's internal regulations for employees formulated according to the law or collective contracts signed according to the law.
c) Consent: Where permitted under applicable local laws, We may (but usually do not) process your Personal Data, Personal Information or Sensitive Personal Data based on your prior freely given consent for one or more specific purposes. In such cases, you have the right to withdraw your consent at any time by contacting the contact details

below provided in this Policy (Section 22). In certain limited circumstances, even after withdrawal of your consent, we may be entitled to continue processing your Personal Data on the grounds of other legal bases and as notified to you. However, in certain jurisdictions, applicable local law may require that consent be obtained and in such circumstances, your consent will be the lawful basis for which we process your Personal Data.

d) Legitimate Interests: We may process your Personal Data and Personal Information where it is necessary for the purposes of our Legitimate Business Interests as a company, including for management purposes, which are outlined above, to prevent and respond to actual or potential fraud or illegal activities, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is under 18 years old. When "legitimate interests" are not a legal basis for processing under the applicable local law, we will rely on your consent.

e) Legal Obligations: We may process your Personal Data and Personal Information where it is necessary in order to comply with applicable legal and/or regulatory obligations, establish, exercise or defend our legal rights or for the purpose of legal proceedings

f) Other "Public Interest" Grounds: We may process your Personal Data, Personal Information (or where relevant, your Sensitive Personal Data) on other public interest grounds where it is subject to regulatory requirements where Processing is necessary by Us for the performance of a task mandated by governmental authorities, regulatory authorities or any other law enforcing authorities in the public interest.

Categories of Personal Data / Personal Information	Purpose of Collection	Legal Basis
LTIMindtree Customer's data/Customer's customer data that is disclosed with	Providing services to fulfil the contractual obligations with LTIMindtree's customers in the role of a Processor. This data will not be	Performance of the contract

LTIMindtree to be processed in the role of a Processor / Sub-processor including identification data; contact information; financial data ; sensitive data (where permitted under local law), information related to your occupation/business activity.	disclosed/processed for any other purpose other than what is stated in the contract between LTIMindtree and its Customers.	
LTIMindtree Customer's data that is disclosed with LTIMindtree to be processed in the role of a Controller including identification data; contact information; financial data ; sensitive data (where permitted under local law), information related to your occupation/business activity.	For sales and marketing, financial, operational activities, administration of information systems, meeting legal obligations and compliance requirements, for all official communication and for all other business purposes.	Legitimate interest of LTIMindtree in order to carry out the contract with the Customer.
Prospective Customers and business partners/ vendors, including identification data, contact data, tax data; financial data;	Maintain and communicate with existing prospective customers, Communication to the prospective customers about LTIMindtree, Conducting Webinars, Sales and Marketing activities.	Consent, Legitimate Interest (when permitted under local laws)

information related to your occupation/business activity.		
Partner/Vendor/Customer Personal Data or Personal Information including identification data, contact data (, tax data; financial data; information related to your occupation/business activity.	Receiving Services from Vendor/ Partner: to receive products and services from you.	Legitimate interest of LTIMindtree in order to carry out the contract with the Partner/Vendor
Personal Data or Personal Information on Prospective Candidates including identification data; contact information; financial data; sensitive data (where permitted under local law).	Employment Opportunities: Where you have applied for a role with us, to review and process your job application with Us and (only where legally permissible and where strictly necessary to assess your suitability for the relevant role) to conduct background screening checks on you (when permitted or required by the applicable law).	Legitimate interest of LTIMindtree for employment opportunities and recruitment purposes/Consent (when legitimate interest is not a legal basis for processing under local laws)
Employee Personal Data or Personal Information including identification data; contact information; financial data; sensitive data	Employment related activities: To carry out activities relating to your employment contract with Us.	Performance of contract, compliance with a legal obligation and legitimate interest of LTIMindtree for

(where permitted under local law).		employment related activities or consen(applicable to Mexico)
Visitor Personal Data or Personal information including identification data; and information related to the purpose of your visit.	Security Purposes: Where you are a visitor to our premises, to record and monitor your use of our premises and/or IT systems in order to maintain their security and protect them against fraud or unauthorised entry.	Legitimate interest of LTIMindtree for security purposes or consent (when legitimate interest is not a legal basis for processing under local laws)
Personal or Personal Information on Data Subjects in the context of Marketing Data, or Website , initiatives, or survey and Events	Marketing purposes: To engage in marketing and business development activities in relation to our products and services. This includes email and SMS marketing, other marketing communications as well as organising events. Use it for our legitimate business interests, such as operating our website, managing the efficient management and operation of our business, conducting marketing activities designed to improve the products and services We offer to you, and administering the security of our business.	Consent, Legitimate Interest to engage in marketing and business development activities in relation to our products and services (when permitted under local laws) of LTIMindtree.

Website Cookies	Marketing purposes: Where you use functionality or visit our website including, subject to acquiring your prior consent where legally necessary, the use of cookies on our website (see our Cookie Policy for more information). https://www.ltimindtree.com/cookie-policy/	Consent, Legitimate Interest (when permitted under local laws)

1 Processing Sensitive Personal Data

We, where legally permissible, process your Sensitive Personal Data on the following lawful bases according to Article 9 of the GDPR:

- Explicit Consent or Explicit Written Consent (where applicable) is obtained from you where required under applicable local laws or in specific circumstances for one or more specified purposes described above (Article 9(2)(a) of the GDPR).
- Where you are physically or legally incapable of giving consent, but the processing is necessary to protect your vital interest (Article 9(2)(b) of the GDPR). For example, where emergency medical care is needed.
- When the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by local Data Privacy Laws or a collective agreement pursuant to local Data Privacy Laws providing for appropriate safeguards for the fundamental rights and the interests of the data subject (Article 9(2)(b) of the GDPR). Please refer to the 'Privacy Notice based on your relationship with us' section of the Data Privacy Policy Statement available here for categories of recipients of Sensitive Personal Data, as applicable to you.

1 Personal Data of Individuals below 18 years

- We process Personal Data or Sensitive Personal Data of any individuals below the age of 18 years only for travel, immigration purposes or when you are visiting our

premises. If we are required to process Personal Data or Sensitive Personal Data of such individuals, then We shall do so by taking explicit consent from their legal guardians and from the minor if they have capacity to give consent, based on their age and maturity. If it comes to your knowledge that We have unintentionally collected or received Personal Data or Sensitive Personal Data about an individual below the age of 18 years directly from them, then please immediately notify Us in the contact details provided in this Policy (Section 22 below) and We will accordingly delete such information.

Note: We do not collect, use nor process Personal data of Individuals below 18 years on our website. If you are below the age of 18 years, then We do not want you to provide any of your Personal Data in our website.

1 Use of Personal Data/ Personal Information in Direct Marketing

For direct marketing, We will be using your Personal Data/ Personal Information in the following ways (to the extent in compliance with applicable local laws).

a) Manage and maintain our relationship with you, including responding to an inquiry, question or comment made by you, as necessary for the relationship between LTIMindtree and the Data Subject;
b) To engage in marketing and business development activities in relation to improving and promoting LTIMindtree's products and services, as necessary for the relationship between LTIMindtree and the Data Subject.
c) To deliver advertising targeted to your interests on other companies' sites or mobile apps;
d) Improve the products and services We offer to you and administering the security of our business.
e) To conduct analysis and market research to improve this website
f) Inform you about our service offerings by communicating through email, SMS, phone and any other similar communications means, as necessary for the relationship between LTIMindtree and the Data Subject.
g) California residents who provide Personal Information are entitled to request information about themselves that We disclosed with Third Parties for their own direct marketing purposes (if applicable), including the categories of information and the

names and addresses of those businesses. We do not currently disclose the Personal Information of California residents to Third Parties for their own direct marketing purposes.

You may "opt-out" of the voluntary purposes of processing at any time by using the means indicated in section 16 "Data subjects' rights".

Where your Personal Data are Processed for direct marketing purposes, you will have the right to object at any time to the processing for such marketing purposes concerning your Personal Data. The Personal Data shall no longer be Processed for such purposes as described in Article 21(2) and (3) of the GDPR.

[To the extent required by applicable law, we will obtain your consent before we pass your Personal Data to any third parties for any marketing purposes.] If you have given us your consent to use your personal data for the above direct marketing purposes, you may opt out and withdraw your consent, free of charge, at any time, by contacting the details below provided in this Privacy Policy. Your opt out will be processed and will take effect as soon as possible.

1. Events and Initiatives

We organize and participate in events and initiatives. In such cases this Policy applies to participants and speakers together with any other supplementary information that is provided in relation with each event. In the event We appoint any Third Parties to conduct or organize such events and initiatives, your Personal Data or Personal Information shall be disclosed to such Third Parties under contractual obligations with such Third Parties in compliance with applicable Data Privacy Laws. The Processing of Personal Data/ Personal Information by such Third Parties shall however be governed by the respective parties' privacy policies and the contractual obligations entered with us.

1 Retention and Disposal of Personal Data or Personal Information

How long we continue to hold your Personal Data/ Personal Information will vary depending principally on:

- Purposes identified in this Policy for using the Personal Data/ Personal Information– We will need to keep the information for as long as is necessary for the relevant purpose; and
- Legal obligations – laws or regulation set a minimum period for which We will have to keep your Personal Data/ Personal Information;
- Disposal of Personal Data/ Personal Information shall be handled with utmost care and shall be governed in accordance with reasonable data security practices as detailed by its internal policies governing data disposal;
- Personal Data/ Personal Information shall only be Processed for the period necessary for the purposes for which it was originally collected as per applicable law and as stated in the LTIMindtree Retention Policy.

1 Cross Border Transfer

We are part of Larsen and Toubro Group (www.larsentoubro.com)which is an international group of companies and, as such, We transfer Personal Data / Personal Information concerning you to countries where LTIMindtree has operations, and in particular to India and USA (where LTIMindtree's SaaS based service providers are present). We transfer Personal Data between our group affiliates companies and data centers for the purposes described above. These data transfers are necessary to provide our products and services. We may also transfer Personal Data on a need-to-know basis to our authorized third-party suppliers, or LTIMindtree customers and authorized business partners.

For Mexico, Your consent may be required unless the transfer is necessary to comply with obligations arising from our legal relationship with you or these third parties are acting as data processors. By providing us with your personal data and using the website/applying for a vacancy or maintaining a legal relationship with us, you agree to the transfer of your personal data where your consent is required. However, you may "opt-out", under certain circumstances, according to the procedure included in section 15 "Rights of data subjects".

Where We transfer your Personal Data/ Personal Information outside of your jurisdiction, We will ensure that it is protected and transferred in a manner consistent with applicable Data Privacy Laws.

For transfers outside the European Economic Area ("EEA"), We ensure that:

We provide adequate protection for the transfer of personal data in accordance with applicable law, by ensuring that:

- the recipient country provides an adequate level of data protection based on the European Commission's adequacy decisions pursuant to Article 45 of the GDPR; or

- the recipient organization has signed a contract based on "standard contractual clauses" approved by the European Commission in its Implementing Decision as referred to in Article 46 of the GDPR, obliging them to protect your Personal Data/ Personal Information. You have a right to request a copy of these Standard Contractual Clauses by contacting Us by using the contact details below (Section 22); and

- where applicable, We have implemented additional (technical, contractual and/organizational) measures to secure the transfer of your Personal Data / Personal Information;
- In the absence of an adequacy decision, pursuant to Article 45(3) of the GDPR, or of appropriate safeguards pursuant to Article 46 of the GDPR, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:
    - (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
    - (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
    - (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

- (d) the transfer is necessary for important reasons of public interest;
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Articles 45 or 46 of the GDPR, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to above is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14 of the GDPR, inform the data subject of the transfer and on the compelling legitimate interests pursued.

For transfers outside the United Kingdom ("UK"), we ensure that:

- the recipient country provides an adequate level of data protection based on the Secretary of State's adequacy decisions pursuant to Article 45 of the UK GDPR; or

- the recipient organization has signed a contract based on "International Data Transfer Agreement" approved by the UK ICO, obliging them to protect your Personal Data/ Personal Information; and

- where applicable, We have implemented additional (technical, contractual and/organizational) measures to secure the transfer of your personal data;
- In the absence of an adequacy decision, pursuant to Article 45(3) of the GDPR, or of appropriate safeguards pursuant to Article 46 of the GDPR, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:
    - (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
    - (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
    - (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
    - (d) the transfer is necessary for important reasons of public interest;
    - (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
    - (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
    - (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

  Where a transfer could not be based on a provision in Articles 45 or 46 of the GDPR, including the provisions on binding corporate rules, and none of the derogations for a

specific situation referred to above is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14 of the GDPR, inform the data subject of the transfer and on the compelling legitimate interests pursued.

For transfers outside Switzerland, We ensure that:

We provide adequate protection for the transfer of personal data in accordance with applicable law, by ensuring that:

- the recipient country provides an adequate level of data protection based on the FDPIC decision and as of September 1, 2023, pursuant to the Ordinnance on the Federal Act on Data Protection ;

- the recipient organization has signed a contract based on "standard contractual clauses" approved by the European Commission in its Implementing Decision as referred to in Article 46 of the GDPR, and the Swiss annex to the standard contractual clauses approved by the FDPIC obliging them to protect your Personal Data/ Personal Information. You have a right to request a copy of these Standard Contractual Clauses by contacting Us by using the contact details below (Section 22); and

- where applicable, We have implemented additional (technical, contractual and/organizational) measures to secure the transfer of your Personal Data / Personal Information;
- In the absence of an adequacy decision, pursuant to Article 45(3) of the GDPR, or of appropriate safeguards pursuant to Article 46 of the GDPR, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of public interest;
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Articles 45 or 46 of the GDPR, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to above is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in

addition to providing the information referred to in Articles 13 and 14 of the GDPR, inform the data subject of the transfer and on the compelling legitimate interests pursued.

For transfers outside of South Africa, we ensure that:

- the recipient organization has signed a contract obliging them to protect your Personal Data / Sensitive Personal Information in a manner that is equivalent or commensurate to the requirements espoused under the Protection of Personal Information Act 4 of 2013; and
- where applicable, we have implemented additional (technical, contractual and/or organizational) measures to secure the transfer of your Personal Data;

For transfers outside the People's Republic of China ("PRC"), we ensure that:

- the recipient organization has signed a contract with LTIMindtree based on "model Standard Contract" released by Cybersecurity Administration of PRC;
- we have obtained your separate consent on the cross-border transfer of Personal Data;
- we have conducted the Personal Information Protection Impact Assessment for cross-border transfer of Personal Data;
- where applicable, the government has approved our application for security assessment on export of Personal Data; and
- where applicable, we have implemented additional (technical, contractual and/organizational) measures to secure the transfer of your personal data;

For transfers outside Australia, we ensure that:

- we notify you of the overseas locations where your Personal Data may be disclosed;
- the third-party recipient of the personal information is located in a territory that has laws or binding rules that protect the personal information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles at Schedule 1 to the Privacy Act protects such personal information and there are mechanisms available to the you to enforce such laws or binding rules; and/or

- take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles.

For transfers outside other jurisdictions, We ensure that:

- there are relevant data processing agreements in line with the applicable Privacy laws signed between its Data exporting branch and its Data importing branch with appropriate responsibilities articulated.

You can obtain more details of the protection given to your Personal Data/ Personal Information when it is transferred outside your jurisdiction (including a sample copy of the model contractual clauses & safeguards) by contacting Us using the details set out within this Policy in Section 22.

1 Security of Personal Data/ Personal Information

In order to comply with our data security obligations under applicable Data Privacy Laws, We have adopted the following physical, technical and organizational security measures to ensure the security of your Personal Data/ Personal Information and PHI, taking into account the applicable industry standards, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for your rights and freedoms:

- That includes the prevention of their alteration, damage, loss, unauthorized processing or access, having regard to the nature of the data and the risks to which they are exposed by virtue of human action or the physical or natural environment.
- We shall comply with the security safeguards as per our contractual and statutory requirements in consultation with its internal I.T department.
- The Office of Data Privacy and Chief Information Security Officer shall assess the security measures implemented to safeguard Personal Data, Personal Information on a regular basis and update the same, where required.
- All employees and contractors shall be imparted with mandatory Privacy training (e.g., Training on Embedding Privacy in Software Development etc.). Further confidentiality

agreements and Non-Disclosure Agreements shall be signed by all employees and contractors on or before their joining date with LTIMindtree.

- We have implemented the following safeguards to ensure the Personal Data We collect, store, process and disclose is secure:
    - Physical Security Controls
        - Facility Perimeter, HD access reader, Data Centre, Video surveillance
    - IT Infrastructure Controls
        - Encryption, DLP, Data masking, controlled Portable ports, Access Control, Unauthorized software check, Data destruction, System Hygiene measures, Monitoring, User Access Management, Patch Management, Vulnerability Management.

We have implemented an incident and breach management procedure to ensure that exceptions in data privacy compliance are promptly reported to the Office of the Data Privacy and to the appointed Data Protection Officer.

1 Privacy by Design

- We have established a process to proactively embed privacy at the initial planning/design stages and throughout the complete development process of new processes/ services/ technologies and/or platforms that involve Processing of Personal Data.

- Considerations have been made for technical and organizational measures to enhance privacy (e.g. pseudonymization, anonymization, data minimization, data aggregation). In addition, We shall take appropriate technical and organizational measures to ensure that Personal Data collected or Processed is adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed.

- With respect to the Personal Information of California residents and in addition to the above, We will use measures to enhance the privacy of your Personal Information through the use of measures to "aggregate consumer information" or to "deidentify" such Personal Information as those terms are defined by the CCPA. Where we take

such measures, we will only process the resulting information in de-identified form and will not attempt to re-identify it except as permitted by law.

1 Rights of Data Subjects

Pursuant to the GDPR, you have the following rights regarding your Personal Data provided for :.

- The right to obtain access to your Personal Data:
  According to Article 15 of the GDPR, you can request a copy of your Personal Data. In particular, you can request information on the purposes of the Processing, the categories of data, the categories of recipients to whom your data has been or will be transferred, the data retention period, the existence of a right of rectification, erasure, limitation of Processing or object, of rectification, erasure, restriction of Processing or object, the existence of a right to lodge a complaint, the source of your data if they have not been collected directly by us, as well as the existence of automated decision-making, including profiling and, if applicable, significant information on its details.
  Please note that according to the GDPR there are circumstances in which We are entitled to refuse requests for access or to receive copies of your Personal Data as in particular cases where such disclosure would adversely affect the rights and freedoms of others.
- The right to obtain rectification of your Personal Data if they are inaccurate or incomplete (Art. 16 GDPR).
- The right to obtain erasure ('right to be forgotten") pursuant to Art. 17 GDPR of your Personal Data: According to the GDPR where one of the following grounds applies, please note that under other circumstances We are legally entitled to retain it:
  - if they are no longer necessary in relation to the purposes for which they were collected or otherwise Processed;
  - if their processing was based on consent and you have withdrawn your consent, and there is no other legal ground for Processing;
  - if the Processing is made for marketing purposes;
  - if you object to the processing on grounds of your particular situation, and there are no overriding legitimate grounds for the Processing;
  - if your data were Processed unlawfully; or
  - your data have been erased for compliance with a legal obligation.
- The right to obtain restriction of the Processing of your Personal Data according to the conditions set out by the GDPR (Art. 18 GDPR).

- The right to object to the Processing of your Personal Data on grounds relating your particular situation, at any time. Where your personal data is processed for direct marketing purposes, you have the right to object at any time to processing of personal data you for such marketing, which includes profiling to the extent that it is related to such direct marketing (Art. 21. GDPR).
- The right to receive your Personal Data provided to Us as a Data Controller in a structured, commonly used and machine-readable format and to transmit that Personal Data to another controller ('data portability')
  According to Article 20 of the GDPR , please note that this right only applies to Personal Data which you have actually provided to us, and when the Processing is based on your consent or on a contract as a legal basis.
- The right to lodge a complaint with the competent data protection supervisory authority, if you think that any of your data protection rights have been infringed by us. To lodge a complaint, please find details provided in Section 22 of this Policy.
- Under article 48 of the French Data Protection Act, data subjects also have the right to set down instructions for the management of their personal data post mortem.

If you need our assistance to exercise the above rights, please contact Us as set out in Section 22 below.

- If the Processing of your Personal Data is based on consent, you can withdraw your consent at any time (Art. 7 (3) GDPR). Your right to withdraw consent can be exercised by contacting Us as set out in Section 22 below. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. In certain circumstances it is lawful for Us to continue Processing your Personal Data without your consent if We have another legal basis (other than consent) for doing so and as notified to you prior to the change of legal basis.

- Right to have onsite access of your Personal Data (for Mexico only).
- Right to raise a request to cancel processing of your Personal Data (for Mexico only)
- Right to limit the use and disclosure of your Personal Data (for Mexico only).

Following are the data subject rights applicable to the respective jurisdictions:

Data Subject Rights	Europe including UK	US	Canada	Mexico	Australia	Singapore	India	UAE	China	Hong-	South

	and Switzerland									Kong	Africa
Right to Information / Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Right to withdraw consent (opt-out)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Right to Object processing	Yes		Yes	Yes			Yes	Yes	Yes		Yes
Right to Restrict processing	Yes		Yes				Yes	Yes	Yes		Yes
Right to Erasure (to be Forgotten)	Yes	Yes	Yes	Yes			Yes	Yes	Yes		
Right to Rectification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Right of Data Portability	Yes	Yes	Yes				Yes	Yes	Yes		
Right not to be subject to automated decision making/profiling	Yes		Yes						Yes		

Right to Complain to the Supervisory authority	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Right not to be subject to discrimination for the exercise of rights	Yes	California Residents	Yes								Yes
Opt-out of sale of data	Yes	California Residents	Yes								
Right to raise a request to cancel processing of your Personal Data				Yes							
Limit the use and disclosure of your Personal Data.				Yes							
Right to have onsite access of your				Yes							

Personal Data											

To exercise the rights outlined above or if you belong to any other jurisdiction that is not listed above in respect of your Personal Data, you may write to dataprotectionoffice@ltimindtree.com with the following information:

- Full Name:
- Email id:
- Data Subject Right you want to exercise:
- Relationship with LTIMindtree (job applicant, student, customer, contractor, employee of LTIMindtree, website visitor, Visitor to LTIMindtree, former employee of LTIMindtree, on behalf LTIMindtree's Data subject, on behalf of a Data subject below the age of 16)
- Country of Residence:
- Request Details:

To receive more details about the applicable procedure and requirements, you may raise a request by contacting dataprotectionoffice@ltimindtree.com

1.1 California Privacy Rights

In the preceding 12 months, we have collected the following categories of Personal Information: identifiers, financial information, health and medical information, demographic information and information relating to protected characteristics, commercial information, biometric information, internet or other electronic network activity information, geolocation data, audio, electronic, and visual information, professional or employment related information, Sensitive Personal Data, and inferences drawn from other information we collect. The categories of sources from which we collect Personal Information are described in Section 5. The business and commercial purposes for collecting Personal Information are described in Sections 6 and 9. In the preceding twelve months we have shared identifiers, internet and other electronic network activity information, and inference information with advertising partners and social media platforms for advertising and other commercial purposes. We have disclosed the categories of Personal Information described above for the purposes and to the categories of recipients identified in Section 17. We do not knowingly share or sell information about individuals younger than 16 and we do not use Sensitive

Personal Data for any purposes that would require us to provide a Notice of the Right to Limit Use of Sensitive Personal Data.

The CCPA provides California residents with the right to request to know more about the categories of Personal Information that the business collects, sells, shares or discloses concerning California residents and We shall provide such information without charge to the requesting California resident after verifying the request. We are required to provide such information no more than twice in a 12-month period. Under the CCPA, "collects" includes information bought, rented, gathered, obtained received and accessed whether actively, passively or by observing the California resident, provided, however, that We are limited in terms of what We can disclose with respect to certain Sensitive Personal Data.

The CCPA requires that We provide data access and data portability to California residents.

Subject to certain exceptions, the CCPA grants rights to California residents to request the deletion of their Personal Information.

The CCPA permits California residents to request that we correct any inaccurate data.
The CCPA permits California residents to opt out of sharing their Personal Information.

The CCPA prohibits discrimination against California residents that elect to exercise their rights under the CCPA.

Please contact the Data Privacy Officer if you are attempting to fulfill any of the above requests by writing to dataprotectionoffice@ltimindtree.com with the following information:

- Full Name:
- Email id:
- Data Subject Right you want to exercise:
- Relationship with LTIMindtree (job applicant, student, customer, contractor, employee of LTIMindtree, website visitor, Visitor to LTIMindtree, former employee of LTIMindtree, on behalf LTIMindtree's Data subject, on behalf of a Data subject below the age of 16)
- Country of Residence:
- Request Details:

California residents who provide Personal Information are entitled to request information about themselves that We disclosed with Third Parties for their own direct marketing purposes (if applicable), including the categories of information and the names and addresses of those businesses. We do not currently share the Personal Information of California residents with Third Parties for their own direct marketing purposes.

For more information, please refer to "LTIMindtree California Privacy Statement."

1 Automated decision making

We do not use your Personal Data to make decisions with legal or similar effects for you, based solely on the automated processing of your Personal Data. In case We will perform automated individual decision-making in the future, We will inform you prior to the processing and we will inform you on your rights, including your right to express your point of view and contest the decision.

1 Disclosure to Third parties

We may disclose some Personal Data/ Personal Information to affiliates within our corporate group under the following circumstances:

- Personnel administration, employee work and business management purposes.
- To provide service that is legally bound by a valid contract.
- To carry out day-to-day business transactions.
- To identify and contact the Data Subject.
- To ensure compliance to local laws and regulations.
- For Security Management purposes.
- Events and Initiatives
- We may also share Personal Data/ Personal Information outside of the corporate group where we rely on Third Parties to assist in its processing activities and we have satisfied legal requirements for such disclosure of the Personal Data.. This includes:
- Third Party agents/suppliers or contractors, bound by obligations of confidentiality, in connection with the processing of Personal Data/ Personal Information for the purposes described in this Policy. This includes IT and communication services providers.
- Third Parties relevant to the products and services that we provide. This includes hardware or software manufacturers, other professional services providers, regulators, authorities and other governmental institutions.

- To the extent required by law, regulatory bodies, enforcement bodies or court order, we may disclose Personal Data/ Personal Information/ Sensitive Personal Data in order to comply with any legal/regulatory obligation. In such instances we might not notify you of such requests, unless permitted by the law.
- Where required for the performance of the role / task of employees of LTIMindtree role, and where permitted or required by applicable laws, business contact details and Personal Data / Personal Information of employees of LTIMindree (Eg: OFCCP data, personal contact details) may be shared with our clients and suppliers.
- Employees may reach out to the contact details provided in Section 29 of this Policy to know the name of the third parties to whom we have shared their Personal Data.
- With respect to disclosing Personal Data/ Personal Information to Third Parties, written contracts and data sharing agreements with Third Parties will include restrictions prohibiting the Third Party from retaining, using or disclosing Personal Data/ Personal Information for any purpose except performing the services specified in the contract or as otherwise permitted by applicable Data Privacy Laws.
- Where it discloses Personal Data/ Personal Information to Third Parties, LTIMindtree will seek to use Data Processors or Sub processors that are capable of providing sufficient guarantees to implement appropriate technical and organisational measures in accordance with applicable Data Privacy Laws and shall put in place contractual mechanisms to ensure that the relevant Data Processor or Sub processor takes reasonable steps to ensure compliance with those measures.
- We have offices and operations in a number of international locations and we share information between our group companies for business and administrative purposes through data processing agreements including the standard contractual clauses signed within the entity.
- Where required or permitted by law, information may be provided to others, such as regulators and law enforcement agencies.
- Where required for your role, and where permitted or required by applicable laws, your business contact details and Personal Data (Eg: OFCCP data, diversity data, personal contact details) may be shared with our clients and suppliers.
- We may also share your resume and background verification status to customers, upon request, to comply with our contractual obligations with these customers (when permitted or required by the applicable law).
- From time to time, we may consider corporate transactions such as a merger, acquisition, reorganization, asset sale, or similar. In these instances, we may transfer or allow access to

information to enable the assessment and undertaking of that transaction. If we buy or sell any business or assets, Personal Data may be transferred to a third parties involved in the transaction.

- To comply with our statutory and other obligations and for the proper management of the LTIMindtree Group, LTIMindtree and our service providers, we may also provide information to other third parties, including, but not limited to, auditors, accountants, lawyers and other professional advisers, as well as to administrative authorities, courts, law enforcement and/or regulatory authorities, arbitrators, experts, adverse parties and/or their advisors. LTIMindtree hereby ensures that in case of sub processing of your Personal Data the obligations that LTIMindtree bears will be contractually reflected in our agreements with our partners, vendors and any other third party.
- LTIMindtree does not sell any Personal Data under any circumstances.

2 Links to Third Party Websites

Our Website may provide links to other Websites, which have their own privacy policies. Such websites will be governed by their respective privacy policies, and you can refer to them to understand how they process Your Personal Information.

Some content or applications, including advertisements on Our Website accessed by You while availing Our services are served by third parties. These third parties may use cookies alone or other tracking technologies to collect information about You when You use their services. The information they collect may be associated with Your Personal Information or they may collect information about Your online activities over time and across different websites and other online services. They may use this information to provide You with interest-based (behavioural) advertising or other targeted content. We do not control these third parties' tracking technologies or how they may use the data which they have accessed. If You have any questions about an advertisement or other targeted content, You should contact the responsible provider/advertiser directly.

2 Quality of Personal Data/ Personal Information Data

- We shall ensure to implement reasonable Processes to monitor the quality of the Personal Data/ Personal Information. We store/ process

- Each business unit & support function within our organisation shall take steps to assure that Processed Personal Data/ Personal Information is complete and accurate and, where necessary, kept up to date.

- We shall implement a process to ensure that our employees can review, update and confirm on the accuracy and completeness of their Personal Data/ Personal Information Processed by us.

2 Managing changes to Data Processing

Except as otherwise described in this Policy, We will only use Personal Data for the purposes described above, or as otherwise disclosed at the time We request such data from you. Should your Personal Data be processed for other purposes than those outlined in this Prvacy Policy, or other purposes than the ones your Personal Data has originally been collected for, We will provide you with information on that other purpose prior to any processing, and provide you with any other relevant information as referred to in this Policy, and when applicable we will collect your consent. Where required by applicable local law, we will obtain your consent before processing your Personal Data for purposes other than those to which you have consented. And to the extent required by applicable local laws, obtain your consent for use of your Personal Data for such other purposes.

2 HIPPA Privacy and Security Requirements

This section describes LTIMindtree's obligations as a Business Associate under the Health Insurance Portability and Accountability Act ("HIPAA").

I. Privacy Officer

LTIMindtree's Data Protection Officer (as specified in Section 22 of this Policy) shall also act as the Privacy Officer and single point of contact for all queries on HIPAA-related matters for LTIMindtree. The Privacy 41Office is also responsible for :

- development and implementation of the policies and procedures pertaining to the protection of PHI and LTIMindtree's obligations thereof;
- compliance with the Privacy Rule;
- establishing a breach notification process and coordinating with the Covered Entity on any breaches;
- developing a training program ; and

- monitoring changes in the law and procedures that affect PHI.

II. Business Associate Agreements

LTIMindtree does not receive, access, use or otherwise process PHI without a Business Associate Agreement (BAA). The BAA ensures that the PHI received from a Covered Entity or Business Associate (hereinafter the LTIMindtree "customer") is properly safeguarded in accordance with the applicable provisions of the HIPAA Privacy Rule, Security Rule, and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). The Privacy Officer shall maintain a log of all BAAs and manage any compliance requirements specified in such BAAs.

Upon termination of a BAA, LTIMindtree will return or destroy all PHI that it received and maintains from the customer, and no copies of such information will be retained. If return or destruction is not feasible, LTIMindtree shall continue to protect such PHI in accordance with the terms of the BAA and applicable law, until such time as the PHI remains in its possession and custody.

III. Use and Disclosure of Protected Health Information

LTIMindtree shall use and disclose PHI solely in accordance with the permitted uses laid out in the Business Associate Agreement between LTIMindtree and its customer, and in compliance with the purposes and standards prescribed under HIPAA.

In the event that a mandatory disclosure request as prescribed in the Act is made directly to LTIMindtree, whether by an Individual, in compliance with a legal directive, or to HHS for the purposes of enforcing HIPAA, LTIMindtree shall, to the extent permitted by law, notify the customer from whom such PHI was received, and shall make the requested disclosure in line with the guidance issued by such customer.

LTIMindtree shall not, in the absence of an authorization from the relevant Individuals, process PHI for any purpose other than the permitted purposes prescribed under applicable law and the BAA; provided however, that the responsibility for obtaining such authorization shall rest solely and exclusively on the LTIMindtree customer on whose behalf such processing shall occur and LTIMindtree shall not, to the extent permitted by law, be liable for any delay or failure by the customer to obtain the requisite authorizations.

IV. Training

LTIMindtree personnel that use, disclose, request, or have access to PHI in order to carry out their work-related functions are required to undergo the prescribed training to permit them to carry out functions in compliance with HIPAA. Training for employees with access to PHI will be pro-vided within a reasonable period of time after their date of assignment to the relevant project. Where applicable, such personnel will be required to take a refresher training annually and at additional times as determined by the Privacy Officer. The Privacy Officer will maintain records of the dates of, and attendance at, all training sessions for six (6) years from the date of the applicable training session.

V. Violations of Policies and Procedures

LTIMindtree takes the policies and procedures regarding PHI very seriously. These policies and procedures are developed and implemented not only to ensure that PHI is used and maintained in a manner that is consistent with LTIMindtree's commitment to privacy and protection of PHI, but also in a manner that is consistent and compliant with its obligations under the BAA and applicable law.

In the event that a LTIMindtree employee fails to comply with their obligations under the abovementioned policies and processes, they may be subject to sanctions, including warnings (verbal or written), and further disciplinary action up to and including termination of employment.

VI. Security Officer

LTIMindtree's Chief Information Security Officer (CISO) shall act as the Security Officer for ensuring compliance with the security obligations prescribed in this section. The Security Officer will coordinate LTIMindtree's security activities with the Privacy Officer. The details of the Security Officer are as follows:

Chief Information Security Officer

_____@LTIMindtree.com

VII. Security Policies and Procedures

LTIMindtree has developed a robust information security framework in line with industry best practices to protect PHI under its control and custody, as detailed in Section 13 above.

2 Contact Details for Complaints and Grievances

If you have any questions, comments, or suggestions, complaints or grievances, of if you want to exercise your privacy rights or wish to raise or consult Us on any privacy issues, our use of Personal Data or Personal Information, you can contacts our appointed Data Protection Officer ("DPO").

Complaints related to Personal Data and Personal Information protection and any communications regarding enforcement of your privacy rights should be directed to the Data Protection Officer at the following contact details:

Global Data Privacy Officer for LTIMindtree Limited:

- Email: dataprotectionoffice@ltimindtree.com
- Address: Data Privacy Office, Gate No. 5, L&T Technology Center, Saki Vihar Road, Powai, Mumbai – 400072
- Attention : Data Protection Officer
- Phone- +91 22 67766776
- Data Privacy Officer for LTIMindtree Limited (Germany Branch) and European Representative

Email ID- dataprotectionoffice.eu@ltimindtree.com

United Kingdom Representative

Email ID - dataprotectionoffice@ltimindtree.com

Switzerland Representative

Email ID - dataprotectionoffice@ltimindtree.com

United Arab Emirates

Email ID - dataprotectionoffice@ltimindtree.com

South African Representative

Email ID - dataprotectionoffice@ltimindtree.com

We will use reasonable efforts to respond your complaint within a reasonable time, usually within 30 days.

You may also raise a concern or lodge a complaint with the competent Supervisory Authority. The name and contact details of the Data Protection Authorities in the European Union can be found here.

You may reach out to the DPO Office (in the above-mentioned contact details) in the event you want a copy of this privacy notice in the local language of European countries where LTIMindtree has an office.

If you are in Australia, and we are unable to satisfactorily resolve your privacy concerns, you can contact the Office of the Australian Information Commissioner on their website www.oaic.gov.au

2 CCTV Surveillance

Where and only as far as permitted by applicable local laws, we may monitor the activities of individuals including visitors in our common area premises through CCTV footage. Such data shall be kept in accordance with LTIMindtree Retention Policy, after considering othser statutory compliance requirements.

2 List of LTIMindtree Entities

We might transfer your personal data to our parent company Larsen & Toubro and its subsidiaries for the purposes as listed in section 17 of this Policy. Please click here to view the list of entities and branches of Larsen and Toubro.

2 Policy Changes and Publication

This Policy was last updated on November 14, 2022.

This Policy may be revised and updated from time to time according to changes in your Personal Data processing. If We update this Policy, We will publish the most recent version on our website in this web page. The modified terms will come into effect immediately upon posting or otherwise notified by Us. You are encouraged to review this Policy periodically for any changes. We will always indicate the date when the last changes were published.

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by more than 85,000 talented and entrepreneurial professionals across 33 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen & Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit www.ltimindtree.com.