DATA PRIVACY POLICY

This Policy is applicable to

L&T Finance Limited

(formerly known as L&T Finance Holding Limited (LTF/Company)

Table of Contents

Preamble

This Data Privacy Policy sets forth the reasonable security practices and procedures adopted by the Company and shall apply to use and disclosure and sharing of Customer's Data on the website/ web application, mobile application or otherwise and in scope includes Cloud IT environment as well ("**Company's information resources**"). This privacy policy shall be read in conjunction with the terms of use agreed by the Customer while registering with Company for availing its Services.

Important Definitions

Customer shall mean any individual who has logged on to Company's Mobile App or Web based application or any other Company's information resource or is a registered user or a borrower of the Company.

Data for the purpose of this Policy (except where specifically defined otherwise) shall mean and include all information and details supplied by the Customer or accessed by the Company or Third Party as per the Consent provided including sensitive personal data/ information that identifies individuals, such as individual's Name, Address, Date of birth, Bank Account details, Phone number, Fax number or Email address.

Services means any of the service(s) that are provided by Company to its Customers and/or users by way of any Company information resources including lending services.

Third Party shall mean and include Company's group entity(ies), third party vendors (of any nature whatsoever) and/or consultants, advisors, partners, banks, financial institutions, credit bureau/ agencies, identity authenticating agencies (NSDL, UIDAI, State Transport Department, etc., regulatory or statutory bodies

(A) Consent

Company shall obtain a Customer's consent in writing or electronically accessed by Company or Third Party as per the Consent provided by the Customer to Access the Data with an audit trail of the purpose/ usage to provide Services under the terms of use. This personal Data collected from Customers is solely for the Purposes provided under this Policy and the Consent provided by the Customer. Access, storage and usage of Data by the Company shall be as permitted/ allowed under extant statutory and regulatory guidelines. For the purpose of this Policy, **'Access'** shall mean and include access, collection, storage, sharing, monitoring.

Data shall be collected on need basis and as provided will be on '*as on basis'*. Company shall not be responsible for unverified personal information or Data supplied by Customers.

Additionally, in case of Digital Lending (as defined under RBI Digital Lending Guidelines, September 2, 2022), Company shall desist from accessing mobile phone resources like file and media, contact list, call logs, telephony functions, etc, except if needed for the purpose of providing Services to Customers or when an express Consent is provided by the Customer. Further, to onboard the Customer through the use of mobile or web application and KYC regulatory requirements, mobile resource access for camera, microphone, location or any other facility necessary, shall be requested from the Customer. Customers have the option to not agree to the collection of Data. Customers can also at any time withdraw the consent and delete/ forget data by uninstallation of the application from the device of the Customer.

(B) Purpose and Usage of Data:

Company requires Customer's Data to operate and provide various Services. Company may Access, share, transfer or use the Data only for the purpose as follows:

1. To fulfill the Customer requests for products and services offered and subscribed and accepted by Customer
2. To deliver to Customer any administrative notices, alerts, advice and communications relevant to Customer's use of the Service

3. Share Customer's Data with any Third Parties in so far as required for purpose of providing additional Services and / or to similar Services to provide Customer with various value-added Services
4. For market research, project planning, troubleshooting problems, detecting and protecting against error, fraud or other criminal activity;
5. To Third-Party contractors that provide services to Company are bound by similar privacy restrictions;
6. Verifying Customer identity and address details and find nearest branches;
7. Enabling secure downloads and uploads of documents related to loan, KYC, otherwise;
8. Managing phone calls and SMS/texts, Sending reminders, etc.;
9. Analyzing Customer's financial position/credit risk assessment/ credit appraisal;
10. "Know Your Customer" (KYC) requirements like verification or authentication (any nature);
11. Data enrichment; Making personalized offers of products and services, credit rating, promotion or marketing of Company's product or its group companies or Third Party.
12. For the purposes connected with Company's 'Terms of Use' on any of the Company information resource;
13. To undertake activities as may be permitted under law/regulations/directions/guidelines or by any authority or under any license or registration of the Company.
14. The Data so collected shall be used only for the purpose otherwise as may be expressly consented by the Customer.
15. All such Data collected shall be retained so long as Customers are having account with Company and remain active to avail various services and/or as may be required under the law or by any authority. In case of deactivation / termination of the account / services with us, the Data provided will no longer be used unless consented for.

(C) Update of Data:

Company encourages the Customers to update this information as and when there are any changes. The Customer is also entitled to review the information provided and ensure that any Data/ personal information found to be inaccurate or deficient be corrected or amended as feasible. However, Company shall not be responsible for unverified, inaccurate or un-updated Data supplied or Accessed from the Customers.

(D) Sharing/Transfer/Disclosure of Data:

Data of the Customers will not be sold or otherwise transferred to unaffiliated third parties except if otherwise stated at the time of collection/Access or under Consent obtained from the Customer or as required under law. However, Company can share, exchange and disclose Data of the Customer to Third Parties with prior consent of the Customer or as may be permitted under applicable laws.

Company treats Customer's Data as private and confidential and does not check, edit, or reveal it to any third parties except as provided under this Policy or where it is expressly agreed and where it believes in good faith, such action is necessary to comply with the applicable legal and regulatory processes or to enforce the terms of service. Company may disclose personal information where it is under legal obligation to do so or where it is mandated under law or directed by any authority. Subject to the provisions of this Policy, Company may transfer Data to another Indian or overseas body corporate that ensures the same level of data protection that is adhered to by the Company, if it is necessary for the performance of a lawful contract between Company or any person on Customer's behalf or where Customer have consented to the data transfer.

Lending Service Providers (as defined under law) or Third Parties are also bound by a contractual obligation to ensure confidentiality of shared data and to comply with various technology standards/ requirements on cybersecurity stipulated by RBI and other authorities, as may be specified from time to time.

Details of Lending Service Providers (where and as applicable) allowed to collect Data through the web-based or mobile application is as available on the website of the Company.

(E) Unsolicited Information:

Except where specifically agreed or necessary for operational or regulatory reasons, Company will not send the Customer any unsolicited information. However, to help the Customer to take full advantage of the service offerings of the Company the Customer will have the opportunity to indicate whether the individual would like to "opt out" of receiving promotional and/or marketing information about other products, services and offerings from Company and/or any Third Parties etc. If the Customer does not opt out, Company may use any email addresses of Customer to send occasional emails pertaining to the said

information. The Customer can nevertheless unsubscribe from receipt of such emails by following instructions therein or by communicating accordingly to Company.

(F) Storage and Retention of Data:

Company shall retain Data of Customer as may be required to carry out their operations under applicable laws/ regulations/licenses or under the Consent provided by the Customer. The Data will be stored only in servers located within India and shall be retained for a period of 10 years from the date it is Accessed or obtained by the Company or so long as Customers are having account with the Company and remain active to avail various services, whichever is later. Subject to as provided in this provision/clause and only if required under any of the applicable laws, Company will purge the Data on the Customer exercising its right to delete/forget the Data or at the end of the tenure of the loan/contract, whichever is later.

(G) Disposal, Destruction and Redaction of Data

Company Data Retention and Disposal require managerial approval for the disposal, destruction and deletion of any Data. Our disposal, destruction and redaction procedures prevent the recovery, theft, misuse or unauthorized access of Data. The same is governed under existing organization's policies/ procedures.

(H) Use of Cookies:

Company's websites may use "cookies" (information stored on an individual's computer by an individual's browser at our request). "Cookies" is a term generally used for small text files a web site can use to recognize repeat users, facilitate the user's ongoing access to and use of the site, allow a site to track usage behavior and compile aggregate data that will allow content improvements and targeted advertising etc. Cookies themselves do not personally identify individuals but they do identify individual's computers or devices. Generally, cookies work by assigning a unique number to the user computer/device that has no meaning outside the assigning site. Users are also being made aware that Company cannot control the use of cookies or the resulting information by advertisers or third parties hosting data on the Company website. If a user does not want information collected through the use of cookies, there is a simple procedure in most browsers that allows the user to deny or accept the cookie feature.

(I) Security of Data

Company is ISO27001:2013 certified and deals with mostly personal identifiable information (PII) of users, it becomes imperative to protect such information as soon as they are in the Company network. The ownership of the data lies with the skilled IT Function Team. Below are the security measures taken to prevent misuse of this type of information.

(1) Company has implemented physical, administrative and technical security measures across the organization which are designed to prevent data loss, unauthorized Access to Data and misuse, disclosure, alteration, damage or destruction of Data.
(2) Sensitive PII data are encrypted at rest using strong encryption algorithms. The keys used for such encryption algorithms are stored securely and access to keys are restricted to authorized entities only.
(3) Company fully understands that the Data collected from individuals is under our guardianship. Therefore, Company trains its employees on the privacy policy as well as information security procedures regarding the appropriate access, use, and disclosure of Data.
(4) Company also conducts periodic risk assessments on the processes and information systems and audits of material third-party vendors dealing with Data of the customer/user.
(5) Company also conducts third party audit & assessment on periodic intervals for material vendors
(6) Company has in place an incident response plan with trained personnel to respond to, investigate and mitigate the impact of any incident.
(7) Company also maintains adequate plans for business continuity management, as well as disaster recovery processes for testing databases, servers, information systems and processes that handle personal data.

This Data Privacy policy shall be read in conjunction with Company Information Security and Information technology policies and procedures, as may be existing and applicable.

(J) Quality

Company informs individuals/users that it is the responsibility of the individuals/ users to provide accurate, complete and relevant information in order to maintain the quality and integrity of the Data available with Company. Individuals/Customer may contact Company designated personnel and have the personal information/Data amended or deleted, as required to ensure accuracy.

(K) Compliance and Reporting

Company is committed to comply with this Policy and with applicable privacy laws, regulations and applicable guidelines from authorities. Company conducts regular audits of our compliance with applicable privacy policies, procedures, laws, regulations, contracts and standards under applicable regulations.

(L) Change in Privacy Policy

Company reserves the right to change Privacy Policy at any time. Users/customers may note that this Policy itself and any such change of Policy will be effective from the date of posting on www.ltfs.com.and shall be considered disclosed to the users/customers.

(M) Grievances:

For any grievances redressal, users/customers may note the redressal process under provided the Grievance Redressal policy available www.ltfs.com.

(N) Protecting Personal data of Aadhar Number Holders:

Subject to obtaining the AUA/KUA license from UIDAI ("the License"), Company will be permitted to directly use the online database of Aadhar to verify the identity of the customers including the photograph seamlessly for the purpose of carrying out the KYC of its customers/borrowers before onboarding. The provisions governing privacy and protection of personal date of the Aadhar Number Holders (Aadhar Holders Personal Data) is detailed under **Annexure A** of this Policy. It may be noted that if any provision(s) of the Policy and Annexure A mean, read or interpreted differently, the provisions of **Annexure A** shall prevail for the purposes of governing the personal data of Aadhar Number Holders.

The **Annexure A** shall stand effective from the date of receipt of the License.

(O) Review / Revision of Policy

If at any point a conflict of interpretation / information between the Policy and any regulations, rules, guidelines, notification, clarifications, circulars, master circulars/ directions issued by relevant authorities ("Regulatory Provisions") arises, then interpretation of the Regulatory Provisions shall prevail. In case of any amendment(s) and/or clarification(s) to the Regulatory Provisions, the Policy shall stand amended accordingly from the effective date specified as per the Regulatory Provisions.

Annexure A

The purpose of this Annexure is to provide direction to the responsible personnel within the Company to protect the personal data of Aadhar number holders in compliance to the relevant provisions of the Aadhar Act, 2016; the Aadhar and Other Laws (Amendment) Act, 2019; the Aadhar (Authentication) Regulations, 2016; the Aadhar (Data Security) Regulations; the Aadhar (Sharing of Information) Regulations, 2016; and the Information Technology Act, 2000, and regulations thereunder.

(A) Definitions:

The below definition will be in continuation any word defined above, however definitions (a) to (r) are only applicable in cases of protection of the personal data of Aadhar number holders.

a) "***Aadhar number***" means an identification number issued to an individual under sub-section (3) of section 3, and includes any alternative virtual identity generated under sub-section (4) of that section.

b) "***Aadhar Data Vault***" ***(ADV)*** means a separate secure database/vault/system where the entities mandatorily store Aadhar numbers and any connected data such that it will be the only place where the said data will be stored.

c) "***Anonymization***" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which an individual cannot be identified, which meets the standards of irreversibility.

d) "***Authentication***" means the process by which the Aadhar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

e) *"**Authentication Service Agency" or "ASA"*** shall mean an entity providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by the Authority.

f) *"**Authentication User Agency**" or "**AUA**"* means a requesting entity that uses the Yes/ No authentication facility provided by the Authority.

g) "***Authority****"* means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Aadhar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

h) "***Biometric information***" means photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations.

i) "***Central Identities Data Repository***" (**CIDR**) means a centralised database in one or more locations containing all Aadhar numbers issued to Aadhar number holders along with the corresponding demographic information and biometric information of such individuals and other information related

j) "***Consent***" means

(1) the personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.

(2) The consent of the data principal shall not be valid, unless such consent is—

(a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;

(b) informed, having regard to whether the data principal has been provided with the information required under section 7;

(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

(e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

(3) In addition to the provisions contained in sub-section (*2*), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained—

(a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;

(b) in clear terms without recourse to inference from conduct in a context; and

(c) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.

(4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

(5) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.

(6) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal.

k) "***Hardware Security Module (HSM)"*** *means a device that will store the keys used for digital signing of Auth XML and decryption of e-KYC response data received from UIDAI.*

l) "***Identity information***" in respect of an individual, includes his Aadhar number, his biometric information and his demographic information.

m) "***Limited KYC***" means the service that does not return Aadhar number and only provides an agency specific unique UID Token along with other demographic fields that are shared with the Local AUAs depending upon its need.

n) "***PID Block***" means the Personal Identity Data element which includes necessary demographic

and/or biometric and/or OTP collected from the Aadhar number holder during authentication.

o) ***"Personal data"*** in respect of and for the purpose of protecting personal data of Aadhar Number holders shall mean the data relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;

p) ***"Personnel***" means all the employees, staff and other individuals employed/contracted by the requesting entities;

q) ***"Processing"*** in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

r) ***Resident***" means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment.

s) *"**Sensitive personal data or information**"* means such personal information which consists of information relating to —

i. password;
ii. financial information such as Bank account or credit card or debit card or other payment instrument details;
iii. physical, physiological and mental health condition;
iv. sexual orientation;
v. medical records and history;
vi. Biometric information;
vii. any detail relating to the above clauses as provided to body corporate for providing service; and
viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise;

provided that, any information that is freely available or accessible in 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 for the purposes of these rules and this Policy.

t) "***UID Token*"** means a 72-character alphanumeric string returned by UIDAI in response to the authentication and Limited KYC request. It will be unique for each Aadhar number for a particular entity (AUA/Sub-AUA) and will remain same for an Aadhar number for all authentication requests by that particular entity.

u) "***Virtual ID (VID)***" means any alternative virtual identity issued as an alternative to the actual Aadhar number of an individual that shall be generated by the Authority in such manner as may be specified by regulations.

1. **Personal Data collection**

   a. Company shall collect the personal data including Aadhar number/Virtual ID, directly from the Aadhar number holder for conducting authentication with UIDAI at the time of providing the services;

2. **Specific purpose for collection of Personal data**

   a) The Identity information including Aadhar number / Virtual ID shall be collected for the purpose of authentication of Aadhar number holder to provide lending service

   b) The identity information collected and processed shall only be used pursuant to applicable law and as permitted under the Aadhar Act 2016 or its Amendment and Regulations.

   c) The identity information shall not be used beyond the mentioned purpose without consent from the Aadhar number holder and even with consent use of such information for other purposes should be under the permissible purposes in compliance to the Aadhar Act 2016.

   d) Process shall be implemented to ensure that Identity information is not used beyond the purposes mentioned in the notice/consent form provided to the Aadhar number holder.

   e) Identity information and Personal Data may be collected and processed by Company to undertake activities permitted under the License and applicable laws.

3. **Notice / Disclosure of Information to Aadhar number holder**

   a) Aadhar number holder shall be provided relevant information prior to collection of identity information / personal data. These may include, as applicable:

      i. The purpose for which personal data / identity information is being collected;

      ii. The information that shall be returned by UIDAI upon authentication;

      iii. The information that the submission of Aadhar number or the proof of Aadhar is mandatory or voluntary for the specified purpose and if mandatory the legal provision mandating it;

      iv. The alternatives to submission of identity information (if applicable);

      v. Details of Section 7 notification (if applicable) by the respective department under the Aadhar Act, 2016, which makes submission of Aadhar number as a mandatory or necessary condition to receive subsidy, benefit or services where the expenditure is incurred from the Consolidated Fund of India or Consolidated Fund of State. Alternate and viable means of identification for delivery of the subsidy, benefit or service may be provided if an Aadhar number is not assigned to an individual;

      vi. The information that Virtual ID can be used in lieu of Aadhar number at the time of Authentication;

      vii. The name and address of the Company collecting and processing the personal data;

   b) Aadhar number holder shall be notified of the authentication either through the e-mail or phone or SMS at the time of authentication and the Company shall maintain logs of the same;

4. **Obtaining Consent**

   a) Upon notice / disclosure of information to the Aadhar number holder, consent shall be taken in writing

or in electronic form on the website or mobile application or other appropriate means and the Company shall maintain logs of disclosure of information and Aadhar number holder's consent.

b) Legal department shall be involved in vetting the method of taking consent and logging of the same, and formal approval shall be recorded from the legal department;

5. Processing of Personal data

a) The identity information, including Aadhar number, biometric /demographic information collected from the Aadhar number holder Company shall only be used for the Aadhar authentication process by submitting it to the Central Identities Data Repository (CIDR).

b) Aadhar authentication or Aadhar e-KYC shall be used for the specific purposes declared to UIDAI and permitted by UIDAI. Such specific purposes shall be notified to the residents / customers / Individuals at the time of authentication through disclosure of information notice;

c) Company shall not use the Identity information including Aadhar number or e-KYC for any other purposes than allowed under RBI regulations or laws applicable to NBFC-ICC or as may be permitted under License and informed to the resident / customers / individuals at the time of Authentication.

d) For the purpose of e-KYC, the demographic details of the individual received from UIDAI as a response shall be used for identification of the individual for the specific purposes of providing the specific services for the duration of the services.

6. Retention of Personal Data

a) The authentication transaction logs shall be stored for a period of two years subsequent to which the logs shall be archived for a period of five years or as per the regulations governing the entity, whichever is later and upon expiry of which period, barring the authentication transaction logs required to be maintained by a court order or pending dispute, the authentication transaction logs shall be deleted;

7. Sharing of Personal data

a) Identity information shall not be shared in contravention to the Aadhar Act 2016, its Amendment, Regulations and other circulars released by UIDAI from time to time.

b) Biometric information collected shall not be transmitted over any network without creation of encrypted PID block as per Aadhar Act and regulations;

c) Company shall not require an individual to transmit the Aadhar number over the Internet unless such transmission is secure and the Aadhar number is transmitted in encrypted form except where

d) transmission is required for correction of errors or redressal of grievances;

8. Data Security

a) The Aadhar number shall be collected over a secure application, transmitted over a secure channel as per specifications of UIDAI and the identity information returned by UIDAI shall be stored securely;

b) The biometric information shall be collected, if applicable, using the registered devices specified by UIDAI. These devices encrypt the biometric information at device level and the application sends the

same over a secure channel to UIDAI for authentication.

c) OTP information shall be collected in a secure application and encrypted on the client device before transmitting it over a secure channel as per UIDAI specifications;

d) Aadhar /VID number that are submitted by the resident / customer / individual to the requesting entity and PID block hence created shall not be retained under any event and entity shall retain the parameters received in response from UIDAI;

e) e-KYC information shall be stored in an encrypted form only. Such encryption shall match UIDAI encryption standards and follow the latest Industry best practice;

f) Company has been classified as a Local AUA by UIDAI and does not store Aadhar numbers of the customers / individuals / residents to maintain their privacy and security;

g) Company (if classified as Global AUAs and KUAs) shall, as mandated by law, encrypt and store the Aadhar numbers and any connected data only on the secure Aadhar Data Vault (ADV) in compliance to the Aadhar data vault circular issued by UIDAI; <*Applicable to global AUAs*>

h) The keys used to digitally sign the authentication request and for encryption of Aadhar numbers in Data vault shall be stored only in HSMs in compliance to the HSM and Aadhar Data vault circulars;

i) Company shall use only Standardisation Testing and Quality Certification (STQC) / UIDAI certified biometric devices for Aadhar authentication (if biometric authentication is used);

j) All applications used for Aadhar authentication or e-KYC shall be tested for compliance to Aadhar Act 2016 before being deployed in production and after every change that impacts the processing of Identity information; The applications shall be audited on an annual basis by information systems auditor(s) certified by STQC, CERT-IN or any other UIDAI recognized body;

k) In the event of an identity information breach, the organisation shall notify UIDAI of the following:

   i. A description and the consequences of the breach;

   ii. A description of the number of Aadhar number holders affected and the number of records affected;

   iii. The privacy officer's contact details;

   iv. Measures taken to mitigate the identity information breach;

l) Appropriate security and confidentiality obligations shall be implemented in the non-disclosure agreements (NDAs) with employees/contractual agencies /consultants/advisors and other personnel handling identity information;

m) Only authorized individuals shall be allowed to access Authentication application, audit logs, authentication servers, application, source code, information security infrastructure. An access control list shall be maintained and regularly updated by organisation;

n) Best practices in data privacy and data protection based on international Standards shall be adopted;

o) The response received from CIDR in the form of authentication transaction logs shall be stored with following details:

   i. The Aadhar number against which authentication is sought. In case of Local AUAs where Aadhar number is not returned by UIDAI and storage is not permitted, respective UID token shall be stored in place of Aadhar number;

ii. Specified parameters received as authentication response;

iii. The record of disclosure of information to the Aadhar number holder at the time of authentication; and

iv. Record of consent of the Aadhar number holder for authentication

but shall not, in any event, retain the PID information.

p) An Information Security policy in-line with ISO27001 standard, UIDAI specific Information Security policy and Aadhar Act 2016 shall be formulated to ensure Security of Identity information.

q) Aadhar numbers shall only be stored in Aadhar Data vault as per the specifications provided by UIDAI.

9. Rights of the Aadhar Number Holder

a) The Aadhar number holder has the right to obtain and request update of identity information stored with the organisation, including Authentication logs. The collection of core biometric information, storage and further sharing is protected by Section 29 of the Aadhar Act 2016, hence the Aadhar number holder cannot request for the core biometric information.

b) Company shall provide a process for the Aadhar number holder to view their identity information stored and request subsequent updation after authenticating the identity of the Aadhar number holder. In case the update is required from UIDAI, same shall be informed to the Aadhar number holder.

c) The Aadhar number holder may, at any time, revoke consent given to Company for storing his e-KYC data, and upon such revocation, Company shall delete the e-KYC data in a verifiable manner and provide an acknowledgement of the same to the Aadhar number holder.

d) The Aadhar number holder has the right to lodge a complaint with the privacy officer who is responsible for monitoring of the identity information processing activities so that the processing is not in contravention of the law;

10. Aadhar Number Holder Access request

a) A process shall be formulated to handle the queries and process the exercise of rights of Aadhar number holders with respect to their identity information / personal data. As part of the process it shall be mandatory to authenticate the identity of the Aadhar number holder before providing access to any identity information.

b) All requests from the Aadhar number holder shall be formally recorded and responded to within a reasonable period.

c) Compliance to the relevant data protection / privacy law (s) shall be ensured.

11. Privacy by Design

a) Processes shall be established to embed privacy aspects at the design stage of any new systems, products, processes and technologies involving data processing of identity information of Aadhar number holders;

b) Company in possession of the Aadhar number of Aadhar number holders, shall not make public any database or records of the Aadhar numbers unless the Aadhar numbers have been redacted or

blacked out through appropriate means, both in print and in electronic form;

c) Before going live with any new process that involves processing of identity information, the organisation shall ensure that Disclosure of information / Privacy notice in compliance to the Aadhar Act 2016 is provided to the resident / customer / individual and that consent is taken and recorded in compliance to Aadhar Act 2016.

d) Quarterly self-assessments shall be conducted to ensure compliance to disclosure of information and consent requirements

e) Privacy enhancing organizational and technical measures like anonymization, de-identification and minimization shall be implemented to make the collection of identity information adequate, relevant, and limited to the purpose of processing.

f) Compliance to the relevant data protection / privacy law (s) shall be ensured.

12. Governance and Accountability Obligations

a) A Privacy committee shall be established to provide strategic direction on Privacy matters

b) A person (Privacy Officer) responsible for developing, implementing, maintaining and monitoring the comprehensive, organization-wide governance and accountability shall be designated to ensure compliance with the applicable laws.

c) The name of the Privacy Officer and contact details shall be made available to UIDAI and other external agencies through appropriate channel;

d) The Privacy Officer shall be responsible to assess privacy risks of processing Identity information / personal data and mitigate the risks;

e) The Privacy Officer shall be independent and shall be involved in all the issues relating to processing of identity information;

f) The Privacy Officer shall be an expert in data protection and privacy legislations, regulations and best practices;

g) The Privacy Officer shall advise the top management on the privacy obligations;

h) The Privacy Officer shall advise on high-risk processing and the requirement of data privacy impact assessments;

i) The Privacy Officer shall act as a point of contact for UIDAI for coordination and implementation of privacy practices and other external agencies for any queries;

j) The Privacy Officer shall be responsible for managing privacy incidents and responding to the same;

k) The Privacy Officer shall also be responsible for putting in place measures to create awareness and training of staff involved in processing identity information, about the legal consequences of data breach to the reputation of the organization;

l) Privacy officer shall ensure that the Authentication operations, systems and applications are audited by CERT-IN (Indian Computer Emergency Response Team), Standardization Testing and Quality Certification (STQC) empaneled auditors or any other UIDAI recognized body atleast on an annual basis;

m) Privacy officer shall conduct internal audits through Data Privacy Officer Office (through Infosec

team) on a quarterly basis and monitor compliance through these audits against Aadhar Act 2016;

n) Privacy officer shall ensure that the front-end operators interacting with Aadhar number holders are trained on a periodic basis to ensure they communicate the disclosure of information to the Aadhar number holder, take consent appropriately after showing the screen to the Aadhar number holder and ensure Security of identity information. Such trainings shall be documented for audit purposes;

o) Aadhar specific trainings to developers, systems admins and other users shall be provided to ensure they are aware of the obligations for their respective roles; Completion of such trainings shall be documented;

p) Privacy officer shall be responsible to formally communicate this policy to all stakeholders and staff who need to comply with this policy; Any changes to the policy shall be communicated immediately;

q) Privacy Officer shall facilitate formal Privacy performance reviews with the relevant stakeholders / Privacy Committee and suggest improvements. The reviews shall consider the results of various audits, privacy incidents, privacy initiatives, UIDAI requirements etc.

13. Transfer of Identity information outside India is prohibited

a) Identity information shall not be hosted or transferred outside the territory of India in compliance to the Aadhar Act and its Regulations.

14. Grievance Redressal Mechanism

a) Aadhar number holders with grievances about the processing can contact the organisation's Privacy Officer via multiple channels like on the website, through phone, SMS, mobile application etc.

b) Reasonable measures shall be taken to inform the residents / customers / individuals about the Privacy Officer and its contact details;

c) The contact details of Privacy Officer and the format for filing the complaint shall be displayed on the organisations' website and other such mediums that are commonly used for interaction with the residents / customers / individuals;

d) Where the medium of interaction is not electronic (such as physical), Poster / Notice board that is prominently visible shall be used to display the name of Privacy officer and contact details;

e) If any issue is not resolved through consultation with the management of the Company, Aadhar number holders can seek redressal by way of mechanisms as specified in Section 33B of the Aadhar Act, 2016.

15. Responsibility for implementation and enforcement of the policy

a) The overall responsibility of monitoring and enforcement of this policy through various mechanisms such as Audits etc. shall be with Chief Information Security Officer

b) Responsibility of the implementation of controls of this policy shall be with Chief Information Security Officer

c) Responsibility of review of Disclosure of information notice, consent clause, method of consent, logging of consent etc. shall be with Legal Head

16. Relevant Provisions of Aadhar Act and Supreme court judgement

a) Following relevant documents shall be referred to for ensuring compliance to the Aadhar requirements:

i. Judgement of Honorable Supreme court dated September 2018

ii. Aadhar Act 2016

iii. Aadhar and Other Laws (Amendment) Act 2019

iv. Aadhar (Authentication) Regulations 2016

v. Aadhar (Data Security) Regulations 2016

vi. Aadhar (Sharing of Information) Regulations 2016

vii. Any other Regulations or notices or Circulars issued by UIDAI from time to time

17. Contact Details

- Name of Privacy Officer: Mr. Mohd Imran
- Phone: 022 62125520
- Email: mohdimran@ltfs.com

Version Control

Version	Date of adoption	Change reference	Owner	Approving authority
1	November, 2023	Adoption of policy by the Board.	Information Security Risk Team	Board of Directors
2	January 2024	Revision - contact information of the Privacy Officer.	Information Security Risk Team	Board of Directors