Data Privacy Policy for Aadhaar based Authentication

Version 1.0

Classification: Public

Contents

1. Purpose

Universal Sompo General Insurance Company Ltd. (henceforth refer as USGIC or Company) recognizes the security of UIDAI information in line with the Aadhaar Act 2016. The confidentiality, integrity, and availability of these shall be always maintained by these partners by deploying security controls in line with the Aadhaar Act 2016, Aadhaar Authentication Application Security Standards.

2. Scope

The Scope of this policy is all departments, employees of the USGIC and partner/vendor who access, process or store Aadhaar related data such as Aadhar number and any other data received from the customers or UIDAI in due course of authentication

3. Policy Clause

3.1 Personal Data collection

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

3.2 Specific purpose for collection of Personal data

a. USGIC shall Identity information including Aadhaar number / Virtual ID shall be collected for the purpose of authentication of Aadhaar number holder to provide.
b. The identity information collected and processed shall only be used pursuant to applicable law and as permitted under the Aadhaar Act 2016 or its Amendment and Regulations.
c. The identity information shall not be used beyond the mentioned purpose without consent from the Aadhaar number holder and even with consent use of such information for other purposes should be under the permissible purposes in compliance to the Aadhaar Act 2016.
d. USGIC shall be implement process to ensure that Identity information is not used beyond the purposes mentioned in the notice/consent form provided to the Aadhaar number holder.

3.3 Notice / Disclosure of Information to Aadhaar number holder

a. Aadhaar number holder shall be provided relevant information prior to collection of identity information / personal data. These shall include:
    1. The purpose for which personal data / identity information is being collected;
    2. The information that shall be returned by UIDAI upon authentication;
    3. The information that the submission of Aadhaar number or the proof of Aadhaar is mandatory or voluntary for the specified purpose and if mandatory the legal provision mandating it;
    4. The alternatives to submission of identity information (if applicable);
    5. Details of Section 7 notification (if applicable) by the respective department under the Aadhaar Act, 2016, which makes submission of Aadhaar 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 Aadhaar number is not assigned to an individual;

6. The information that Virtual ID can be used in lieu of Aadhaar number at the time of Authentication;
7. The name and address of the USGIC collecting and processing the personal data;

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

3.4 Obtaining Consent

a. Upon notice / disclosure of information to the Aadhaar number holder, consent shall be taken in writing or in electronic form on the website or mobile application or other appropriate means and USGIC shall maintain logs of disclosure of information and Aadhaar 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;

3.5 Processing of Personal data

a. The identity information, including Aadhaar number, biometric /demographic information collected from the Aadhaar number holder by USGIC shall only be used for the Aadhaar authentication process by submitting it to the Central Identities Data Repository (CIDR).
b. Aadhaar authentication or Aadhaar 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. USGIC shall not use the Identity information including Aadhaar number or e-KYC for any other purposes than allowed under 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.

3.6 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;

3.7 Sharing of Personal data

a. Identity information shall not be shared in contravention to the Aadhaar 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 Aadhaar Act and regulations;
c. USGIC shall not require an individual to transmit the Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances;

3.8 Data Security

a. The Aadhaar 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. Aadhaar /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. USGIC shall store e-KYC information in an encrypted form only. Such encryption shall match UIDAI encryption standards and follow the latest Industry best practice;
f. USGIC has been classified as a Local AUA by UIDAI and does not store Aadhaar numbers of the customers / individuals / residents to maintain their privacy and security;
g. The keys used to digitally sign the authentication request and for encryption of Aadhaar numbers in Data vault shall be stored only in HSMs in compliance to the HSM and Aadhaar Data vault circulars;
h. USGIC shall use only Standardization Testing and Quality Certification (STQC) / UIDAI certified biometric devices for Aadhaar authentication (if biometric authentication is used);
i. All applications used for Aadhaar authentication or e-KYC shall be tested for compliance to Aadhaar 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;
j. In the event of an identity information breach, the organisation shall notify UIDAI of the following:
    1. A description and the consequences of the breach;
    2. A description of the number of Aadhaar number holders affected and the number of records affected;
    3. The privacy officer's contact details;
    4. Measures taken to mitigate the identity information breach;
k. 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;
l. 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;
m. Best practices in data privacy and data protection based on international Standards shall be adopted;
n. The response received from CIDR in the form of authentication transaction logs shall be stored with following details:

1. The Aadhaar number against which authentication is sought. In case of Local AUAs where Aadhaar number is not returned by UIDAI and storage is not permitted, respective UID token shall be stored in place of Aadhaar number;
2. Specified parameters received as authentication response;
3. The record of disclosure of information to the Aadhaar number holder at the time of authentication; and
4. Record of consent of the Aadhaar number holder for authentication but shall not, in any event, retain the PID information.

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

p. Aadhaar numbers shall only be stored in Aadhaar Data vault as per the specifications provided by UIDAI.

3.9 Rights of the Aadhaar Number Holder

a. The Aadhaar 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 Aadhaar Act 2016, hence the Aadhaar number holder cannot request for the core biometric information.

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

c. The Aadhaar number holder may, at any time, revoke consent given to USGIC 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 Aadhaar number holder.

d. The Aadhaar 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;

3.10 Aadhaar Number Holder Access request

a. A process shall be formulated to handle the queries and process the exercise of rights of Aadhaar 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 Aadhaar number holder before providing access to any identity information.

b. All requests from the Aadhaar 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.

3.11 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 Aadhaar number holders;

b. The USGIC, in possession of the Aadhaar number of Aadhaar number holders, shall not make public any database or records of the Aadhaar numbers unless the Aadhaar 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 Aadhaar Act 2016 is provided to the resident / customer / individual and that consent is taken and recorded in compliance to Aadhaar 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.

3.12 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) empanelled auditors or any other UIDAI recognized body at least on an annual basis;
m. Privacy officer shall conduct internal audits (through internal audit team) on a quarterly basis and monitor compliance through these audits against Aadhaar Act 2016;
n. Privacy officer shall ensure that the front-end operators interacting with Aadhaar number holders are trained on a periodic basis to ensure they communicate the disclosure of information to the

Aadhaar number holder, take consent appropriately after showing the screen to the Aadhaar number holder and ensure Security of identity information. Such trainings shall be documented for audit purposes;

o. Aadhaar 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.

3.13 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 Aadhaar Act and its Regulations

3.14 Grievance Redressal Mechanism

a. Aadhaar number holders with grievances about the processing can contact the 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 USGIC's 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 USGIC, Aadhaar number holders can seek redressal by way of mechanisms as specified in Section 33B of the Aadhaar Act, 2016.

f. The Aadhaar number holder can visit https://www.universalsompo.com/resourse-grievance-redressal to know the Grievance redressal mechanism of USGIC and for raising a complaint.

3.15 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 Risk Officer

b. Responsibility of the implementation of controls of this policy shall be with Information Security Risk Management Committee

c. Responsibility of review of Disclosure of information notice, consent clause, method of consent, logging of consent etc. shall be with Chief Compliance Officer

3.16 Relevant Provisions of Aadhaar Act and Supreme court judgement

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

1. Judgement of Honorable Supreme court dated September 2018
2. Aadhaar Act 2016
3. Aadhaar and Other Laws (Amendment) Act 2019
4. Aadhaar (Authentication) Regulations 2016
5. Aadhaar (Data Security) Regulations 2016
6. Aadhaar (Sharing of Information) Regulations 2016
7. Any other Regulations or notices or Circulars issued by UIDAI from time to time

3.17 Contact Details

- Name of Privacy Officer: Mrs. Aarti Kamath
- Email: privacyofficer@universalsompo.com