HYPERVERGE SERVICES PRIVACY POLICY-PROCESSOR

1. Summary

This HyperVerge Services Privacy Policy- Processor ("**Services Privacy Policy**") explains how HyperVerge Inc. and HyperVerge Technologies Private Limited, ("**HyperVerge**", "**we**", "**us**", "**our**") uses, shares, collects and transfers personal information about its clients' users, and others, to provide Services to clients.

HyperVerge helps entities verify their users by carrying out checks related to an identity, or provide user authentication services ("**Services**"). This policy outlines how HyperVerge, as a service provider and processor to the client, processes user's personal information, to provide Services to a client.

2. Applicability

This Services Privacy Policy applies to HyperVerge's clients and their end users ("you", "your").

3. Client Privacy Policies

If you are an end user of HyperVerge's client, HyperVerge uses your information to provide services, as a service provider on behalf of a client. The client, as the business/data controller, may have additional obligations under applicable law, including the California Consumer Privacy Act, and we suggest you review their privacy policy for further details. The client is responsible for identifying a legal basis which permits your personal information to be processed, stored, shared for the purposes of providing Services to the client.

4. Updates

Any updates, modifications, revisions or amendments to this Privacy Notice shall be published herein from time to time.

5. What information is collected?

HyperVerge collects, processes and stores the following personal information about the client's users on behalf of the client to verify the client's users identity or carry out related checks:

(a) **Personal Information**: Such information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, which includes, the following:

- (i) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, other national identity number, driver's license number, passport number, proof of address documents, or other similar identifiers;
- (ii) User's video or image;
- (iii) Biometric information;
- (iv) Internet or other electronic network activity information;
- (v) Geolocation data;
- (vi) Audio, electronic, visual, thermal, olfactory, or similar information;
- (vii) Professional or employment-related information;
- (viii) Education information;
- (ix) Information extracted from documents submitted by the user, including information extracted from the security chip embedded in the document;

(x) Information extracted from a user's identity document, utility bill, including document number, date of birth, nationality, type of document, issuing country, expiration date, information embedded in barcodes, QR codes, security chips and features, photo, and any image metadata associated with the image or video of the document;

(xi) Bank statement, salary slip;

(b) **Sensitive Personal Information:** Including the following following non- public information:

(i) A user's social security, driver's license, state identification card, or passport number;

(ii) A user's precise geolocation;

(iii) A user's racial or ethnic origin, citizenship or immigration status, or union membership, as evidenced from identification card or other information provided by the user;

(c) **Biometric Information**: The processing of biometric information for the purpose of uniquely identifying a consumer, i.e. data from photos/videos of user and user's identity documents captured via user's device camera or otherwise uploaded, including data that may be construed as a scan of face geometry extracted from such images/videos of user and user's identity documents submitted to HyperVerge or the client.

6. How information is collected and processed?

(a) Source of information: Such personal information about a user is collected from:

(i) the client;

(ii) the user itself through the client's platform/ app;

(iii) public authorities or government websites/databases to authenticate or fetch user's information; or

(iv) authorised third party data providers.

(b) Identification document verification: HyperVerge's models analyze the authenticity of the document, which may include machine-readable zones, barcodes, QR codes, and security chips, to verify whether the document is genuine or shows signs of tampering.

(c) Biometric information: HyperVerge generates two scans of the user's face: (i) one from the image provided by the user (such as a selfie), and (ii) one from the reference image (such as in user's identity document) and compare those two scans to assess whether the person in the image is likely to be the same person pictured in the reference image.

(d) Verification checks: To compare user's personal information with third party databases, including voter and driving license registers, government databases, consumer credit agencies, sanctions and Politically Exposed Persons (PEP) lists, anti money laundering (AML) and Know Your Client (KYC) requirements, adverse media sources, utility companies, mobile network providers and other trusted commercial sources.

(e) Fraud Prevention or prior-engagement checks: If required by the client, HyperVerge may use user's personal information to determine if (i) the client has previously engaged with a user; (ii) an image, photo, device, email address or phone number has previously been used in relation to suspected fraudulent activity, shows unusual usage patterns, has been manipulated or otherwise indicates that the user may not be genuine.

(f) Training models for the client: If specifically required by the client, HyperVerge may use the user's personal information to train HyperVerge's models to recognise a new version of an ID document, to minimize bias and improve performance. We rely on the client to obtain consent from the user to enable such training.

(g) Support Services to Client: Providing debugging, error analysis or support services to the client in relation to user's onboarding/authentication/verification.

(h) HyperVerge Service Results: HyperVerge service results may contain confidence score, recommendations and the reasons behind them. Basis this, the client independently decides to move ahead with a user in combination with other information available with the client. HyperVerge does not undertake any credit decisions or decisions that produce legal or similarly significant effects concerning the user, on behalf of the client.

(i) Disclosure to Government: HyperVerge may disclose user's personal information in response to a request from enforcement body, regulatory, government agency, or court, to ensure compliance with legal obligations under applicable law.

7. Information sharing

In addition to sharing personal information with clients HyperVerge also shares personal information with the following:

(a) Third-party service provider: Third party service providers/sub-processors which help HyperVerge provide Services to the client, pursuant to contractual relationships. Such class of service providers/sub-processors includes cloud service provider, information technology provider, infrastructure providers, data analytics providers, outsourcing partners, artificial intelligence companies, and database providers;

(b) HyperVerge group companies: In case of HyperVerge Inc., with HyperVerge Technologies Private Limited, which helps HyperVerge Inc. to provide Services, including for providing engineering, technical, infrastructure, manpower or customer support;

(c) Auditors and lawyers: With parties that provide HyperVerge with professional advice and services;

(d) Government database: With official government database, including police or other authority records, to fetch corresponding verification or personal information of user;

(e) Governmental authorities: With law enforcement body, regulatory, government agency, or court, to ensure compliance with legal obligations under applicable law;

8. Security

Personal information is safe with HyperVerge. HyperVerge uses robust industry standards of care to store, transmit, and protect such data from disclosure, in a manner that is the same as or more protective than the manner in which HyperVerge stores, transmits, and protects other confidential and sensitive information. HyperVerge also takes appropriate administrative, physical, technical and organizational measures designed to help protect the information it holds from loss, theft, misuse and unauthorized access, disclosure, alteration and destruction. When sharing data with third party service provider/sub-processors or group companies, HyperVerge protects the personal information by imposing contractual privacy and security safeguards on the recipient of that information.

9. Storage

(a) HyperVerge stores personal information for such period as is contractually required by the client for providing Services or maximum period permitted under applicable law, whichever is lesser. Thereafter, the data is securely deleted.

(b) However, HyperVerge may store personal information for longer on receipt of a binding legal correspondence from governmental, statutory authority or a court of law. Thereafter, the data is securely deleted.

10. CLASS ACTION WAIVER

TO THE EXTENT PERMISSIBLE BY LAW, ALL PAST, PRESENT, AND FUTURE LEGAL DISPUTES AND LEGAL CLAIMS BETWEEN THE USER AND HYPERVERGE THAT ARE NOW IN EXISTENCE OR THAT MAY ARISE IN THE FUTURE, INCLUDING, BUT NOT LIMITED TO LEGAL DISPUTES OR LEGAL CLAIMS ARISING OUT OF OR RELATING IN ANY WAY TO THIS SERVICES PRIVACY POLICY, OR THE SERVICES, AND ANY FEDERAL, STATE, OR LOCAL STATUTE, LAW, RULE, REGULATION OR ORDINANCE APPLICABLE TO THE RELATIONSHIP BETWEEN THE USER AND HYPERVERGE AS TO WHICH A COURT WOULD BE AUTHORIZED BY LAW TO GRANT RELIEF IF THE CLAIM WERE SUCCESSFUL (“**DISPUTE**” OR “**DISPUTES**”) WILL BE CONDUCTED SOLELY ON AN INDIVIDUAL BASIS. THE USER WILL NOT SEEK TO HAVE ANY DISPUTE HEARD AS A CLASS ACTION OR IN ANY OTHER PROCEEDING IN WHICH THE USER ACTS OR PROPOSES TO ACT IN A REPRESENTATIVE CAPACITY. NO PROCEEDING WILL BE COMBINED WITH ANOTHER WITHOUT THE PRIOR WRITTEN CONSENT OF ALL PARTIES TO ALL AFFECTED PROCEEDINGS. THE USER AGREES NOT TO PARTICIPATE IN CLAIMS BROUGHT IN A PRIVATE ATTORNEY GENERAL OR REPRESENTATIVE CAPACITY, OR ANY CONSOLIDATED CLAIMS INVOLVING ANOTHER PERSON'S ACCOUNT, IF HYPERVERGE IS A PARTY TO THE PROCEEDING. THE USER IS GIVING UP ITS RIGHT TO PARTICIPATE AS A CLASS REPRESENTATIVE OR CLASS MEMBER ON ANY CLASS CLAIM THE USER MAY HAVE AGAINST HYPERVERGE INCLUDING ANY RIGHT TO CLASS ARBITRATION OR ANY CONSOLIDATION OF INDIVIDUAL ARBITRATIONS.

11. Contact Data Protection Officer

(a) For any security vulnerability or, please report it to **dpo@hyperverge.co**

(b) If the user would like more information about how HyperVerge collects and uses personal information, please contact HyperVerge at **dpo@hyperverge.co** or at:

“Attention: Data Protection Officer
Address: HyperVerge, No. 12, 2nd Floor, Urban Vault, 17th cross, Sector 7, HSR Layout, Bengaluru
Karnataka, India, 560102.”