Data Protection Policy

This data protection policy (hereinafter: “**Privacy Policy”**) informs you of our privacy practices regarding Vereign for Gmail and Vereign for Outlook (MS Office 365) and any services we are providing with the help of the applications, referencing this policy (hereinafter: “**Vereign Services”**).

I. Name and contact details of the controller

Vereign AG

Kolinplatz 10,

6300 Zug, Switzerland

Email: contact@vereign.com

For questions with regard to this Privacy Policy or other concerns in this subject area, you may contact our data protection team by email directly via: dataprotection@vereign.com.

II. General information

At Vereign we respect your personal data. Naturally, our data protection practice complies with applicable law including but not limited to the Swiss Data Protection Act (“**Swiss DPA**”) and its Ordinance (“**Swiss DPO**”). Also we are fully compliant with the General Data Protection Regulations (“**GDPR**”) of the European Union and its local adaptations including but not limited to the German Federal Data Protection Act (“Bundesdatenschutzgesetz”). We will continue to monitor and analyse further country specific data protection regulations outside of the European Union but so far we have identified the GDPR as sufficient and acceptable regulatory standard throughout the entire world.

As a matter of principle, we collect and use personal data as much as necessary to provide our services requested by you (Art. 6 para. 1 Lit. b GDPR). A notable exception applies where a contractual basis is not apparent and the processing of personal data can only be authorised via your explicit consent (Art. 6 para. 1 Lit. a GDPR). In such a situation we will explain to you the exact purposes and consequences of the concerned data processing and you may at any time retrieve your consent given to us. In no event will we sell your personal data to any third party for any business or political agenda.

III. Allowed purposes for collecting and processing your personal data

Our collection and processing of your personal data under this Privacy Policy is limited to the extent necessary to fulfil the following purposes:

1. Sender Audit-Log

In order to provide you and your recipients with a tamper-proof verification and evidence of your send email, we have established two channels of data processing and storing:

a) E-Mail Metadata:

Provided you choose to send an email with our Vereign Services activated the following email metadata will be collected:

- Your name and email address

- Subject of the message

- Name and email of all recipients (to and cc)

- Date of the message

- The names (links), size and signature of the attachments (if any)

- Hash and size of the message body

- Status ID

- Your Vereign public key (UUIDv4)

(hereinafter collectively: “**Metadata**”)

To increase the security of your Metadata we have implemented a form of pseudonymization of your personal data, which is part of our privacy by design concept. We are encrypting, compressing and subsequently shredding this Metadata in random pieces. One part of the data output is stored exclusively in the QR code itself which is part of your sent email (hereinafter: “**QR Component**”). The other part is stored in a resilient cloud environment (hereinafter: “**Cloud Component**”).

None of these two random data pieces alone can be restored into your original Metadata. Only in case the Cloud Component is united with the missing pieces of information in the QR Component, it is technically feasible to restore and authenticate your Metadata.

This means it will only be feasible for us (or anyone else) to present your Metadata to someone already having access to your respective email, which by-itself already contains all the data elements of the respective Metadata.

b) Hashes

In order to provide your recipients (and yourself) with an absolutely tamper-proof audit-trail regarding your email, we are using cryptographic hash functions. Such hash functions are widely used to mathematically proof that an original data input has not been altered. As long as the hash input is complex enough, the hash output by itself is an abstract piece of information and will not reveal any information of the original data input itself.

We are mathematically obfuscating the following data input objects via such a hash function:

- Entire message body

- Attachments of the email (if any)

(hereinafter **"Sender Input Data")**

Together with multiple other hash outputs, your respective abstract hash is written in a system data container object and these objects are stored in a resilient cloud environment (hereinafter: "**Data Container Objects**"). Your abstract data hash is secured by your QR Component, meaning without having access to your QR Component, nobody has access to the hash and to its confirmational value in regards to your Sender Input Data.

As an additional security feature in order to safeguard an absolutely tamper-proof audit trail, we are writing hashes of these already hashed system data containers to a public Blockchain network administrated by Æternity Establishment.

Given the complexity of the hashed data, the Data Container Objects but even more so the resulting Blockchain entry is practicable infeasible to invert, without having access to your Sender Input Data anyway.

2. Receiver Audit-Log

While using our Vereign Services, for any email send by another user of our Vereign Services the sender will receive an automatic acknowledgement of receipt, as soon as the mail as been received by your email account. This is a comparable function as you may have seen in popular instant messengers.

For this functionality we are hashing the following information:

- Confirmation of receipt (check-mark you have received the mail)

- Hash of the emailaddress of recipients

(hereinafter "**Recipient Input Data"**)

This hash of Recipient Input Data is encrypted with the public key of the sender and stored again in in a resilient cloud environment and finally on a public blockchain, just as described in no. 2 above for the Sender Input Data.

3. Customer care

As long as you choose to continue to use our Vereign Services we will keep you informed about our software development and additional Vereign services and features. Also we may may ask about your user experience and other relevant feedback. For these reasons, we might reach out to you by using the applications (extensions, add-ins) that are providing you with the Vereign Services.

Regardless of the channel you use to provide us with your feedback, as an open source company your collaboration and engagement is crucial for us. We need interested participants to test and try out the Vereign Services and provide us with feedback. If you choose to engage in such software testing and providing us with feedback, in the spirit of the free software community, this is also a main reason you are providing your personal data to us and this purpose forms our legal relationship in the meaning of Art. 6 para. 1 Lit. b GDPR. We commit ourselves to exclusively use your related personal data for this purpose of testing and improving Vereign Services.

IV. Data erasure and storage period

1) Email Metadata

As explained above your QR Component is exclusively stored in the QR code as attached to your emails (stored in your email send folder and in the email inbox of any of your recipients). We have no technical access whatsoever (and no intention) to erase these emails from the respective email accounts. But naturally, you may at any point in time arrange for the deletion of any of the distributed copies of the QR Component with your chosen recipients. As soon as you accomplish such a complete deletion of the distributed QR Components, your Sender Input Data and Metadata will be barred from access permanently. But please note, we have no way of identifying the recipients you sent the QR Code to.

We will keep the corresponding pseudonymous QR Lock for a period of 10 years (erase process will be done once a year at the end of calendar year). Before this period of 10 years has elapsed, a request to block this data from future access to authenticate and validate the respective email, will require a written substantiation of your legitimate interest. Furthermore your request for blocking access, will need to be documented by us (in case one of your recipients is later demanding an explanation why the authentication value of the QR Component is no longer available to them).

2) Hashes

a) of the Sender Input Data

As long as a copy of your sent email (including the QR Component) exists, the hashes (in the Data Container Object just as on the Blockchain) will provide an additional layer of reliable evidence that your Sender Input Data is authentic and has not been altered. But by itself the Data Container Objects (just as the subsequent Blockchain hash) is just a seemingly random sequence of characters discoverable by an abstract one time transaction identifier. That means, after all copies of your email (and QR Component) has been erased, the abstract hashes in the Data Container Objects and in consequence also the Blockchain hashes will have no counterpart and will consequently bear no significance whatsoever.

But please note, in case you have chosen to share your email (and QR Component) with other recipients, these recipients will be technically able to join the QR Component together with the hashes and thereby may access the conformational value of the stored hash. Same applies, in case your recipients share the QR Code with others. This even applies in case a recipient forwards your information to others without your consent. However please understand, even though such a forwarding may constitute a breach of your confidence, this is excursively a matter between you and your recipients of communication. In particular please note, anyone having access to your email (legitimately or illegitimately) will already have access to all of your actual Sender Input Data contained in that email.

The corresponding Data Container Object will be kept by us for a period of 10 years (erase process will be done once a year at the end of calendar year). After the Data Container Object is erased the hash on the Blockchain will have no counterpart and will consequently bear no significance whatsoever. Thereby it is technically feasible to separate your personal information from the abstract hashes, leaving the hashes without relevance for you and any of your personal information.

The abstract Blockchain hash itself is written on a public Blockchain, which very essence and reason for existence is to provide a permanent and tamper-prove record, that technically cannot be manipulated or erased by anyone (including us). But the confirmatory value of the Blockchain hash will cease to exist in that moment in that either any copies of the QR Component or the corresponding hashed Data Container Object itself is erased.

b) of the Recipient Input Data

Just as the Sender Input Data, the Data Container Object containing the hash of the Recipient Input Data will be kept by us for a period of 10 years (erase process will be done once a year at the end of calendar year)

After the Data Container Object is erased also the confirmatory value of the Blockchain hash will cease to exits, and the hash is left as an abstract mathematical output, without any relevance for you (or anyone else).

V. Data processors

The administration and processing of personal data in the scope of this Privacy Policy is primarily carried out by us, and our subsidiary Vereign Labs Ltd. (a Bulgarian company, having its registered office address at ul. Brezovska 36 et.4-15, BG-4003 Plovdiv, Bulgaria).

However, for specific tasks, like storing your QR Lock in an resilient data center environment, we also have contracted external service providers.

Any of such external providers, just as our subsidiary, are processing your personal data on our behalf. All these parties remain contractually and legally bound to this privacy policy and any applicable law, including but not limited to GDPR.

VI. Rights of the data subject

According to applicable law (in particular Swiss law and even more so GDPR) but also due to our own commitment you shall have the following rights toward us:

1. Right of access: You may request information about your data processed by us, in particular about the purposes of processing, the category of personal data, the categories of recipients to whom the data have been or will be disclosed by us, the envisioned period of storage, the existence of a right of rectification, erasure, restriction of processing or objection to it, the existence of a right to lodge a complaint, where your data are collected from (if these are not collected by us), and the existence of automated decision-making, including profiling.

2. Right to rectification: You have the right to demand without undue delay the rectification of inaccurate personal data stored by us as well as to have incomplete personal data stored by us completed.

3. Right to erasure: You have the right to demand that personal data stored by us be erased as long as the processing of this data is not necessary to fulfil a legal obligation, for reasons of public interest, or for the establishment, exercise or defence of legal claims.

4. Right to block data: You have the right to demand to have your personal data blocked. Data that is blocked will not be deleted from our databases, but it will not be processed as long as being blocked.

5. Right to data portability: You have the right to receive your personal data in a structured, commonly used and machine-readable format, or to demand that it be transmitted to another controller.

6. Right to object: Consent given to process your personal data can be revoked at any time. As a result of this, we will no longer be permitted to continue processing data based on this consent in the future.

7. Right to lodge a complaint: You have the right to lodge a complaint with any competent supervisory authority. Therefore you may contact a locally competent authority at your place of residence or you may report any presumed violation of applicable data protection law, to the Federal Data Protection and Information Commissioner (FDPIC) as the federal data protection authority in Switzerland. The FDPIC’s contact details are as follows:

Federal Data Protection and Information Commissioner

Feldeggweg 1, 3003 Berne, Switzerland

Tel: +41 58 462 43 95

Fax: +41 58 465 99 96

www.edoeb.admin.ch

8. Exercise your rights

In order to exercise your rights as a data subject, please contact our Data Protection Team (dataprotection@vereign.com) or send an email or postal mail to our contact details as indicated under clause I above.

In case you exercise your rights in accordance with the GDPR towards us, we will not charge any fees. However, a reasonable fee may be charged if your inquiry is demonstrably abusive, improper or if you make a repeated inquiry without relevant justification.

We may need to collect information about you that will enable us to clearly identify you as a data subject. In doing so, we will endeavour not to complicate or even hinder your request. Rather, we want to make sure that none of your personal data falls into the hands of unauthorised persons.

VII. Security

We have implemented extensive security provisions and measures to establish an appropriate level of safety to protect personal data stored by us from unauthorized access, misuse, altering, misappropriation, destruction, and loss.

However, in case you choose to communicate with us via an insufficiently encrypted communication channel, we would like to point out that such insufficiently encrypted data transfer via the internet cannot provide any guarantee that access to your data by third parties is averted. Adequate protection of your data during unencrypted transfer from your system to our server is not possible in technical terms.

VIII. Amendments of this Privacy Policy

It may be necessary to adapt our data protection statement to changing framework conditions of a technical, factual or legal nature. This Privacy Policy may be amended from time to time.

As of: October 2020