Data Protection Policy

At Vereign we respect your personal data. In this spirit, this data protection policy (hereinafter: “Privacy Policy”) shall offer you full transparency on how we protect your data.

In detail this Privacy Policy applies to Vereign for Gmail, Vereign for Outlook (MS Office 365), our web application which is opened in your browser after you clicked or scanned our QR code seal (hereinafter collectively: “Seal Applications”) and any services we are providing with the help of these Seal Applications (hereinafter: “Vereign Services”).

I. SUMMARY OF OUR COMMITMENTS

✔ Our Vereign Services empower you to add and verify privacy-secured seals of authenticity, directly in your email inbox. Such seals of authenticity prevent impersonation just as well as falsified emails (hence offers effective protection from impersonating scam or so called “Phishing”). Furthermore you are provided with reliable evidence, in case of future disagreements. For more information see https://www.vereign.com/#how-it-works.

✔ Our Vereign Services are equipped with a strong privacy by design concept. Consequently, for sealing or verifying a sealed email, only (by itself) abstract data like shredded data and hashes are collected and subsequently processed on remote servers.

✔ The actual meaning of such abstract remote data will only be accessible in case your corresponding email is present. As long as you (or your recipients) do not send us such a matching and sealed email, even we cannot make sense of the abstract remote data.

✔ Only in case you have explicitly subscribed to our Vereign Services, as our customer, we will process your actual user data in the form of your user account information - you have explicitly provided to us, for the sole purpose of administrating your subscription.

✔ In no event we will use your personal data for any purpose unrelated to our Vereign Services. In particular, we are not allowed to sell your personal data to any third party for any business or political agenda.

Nothing in the following detailed explanations shall put this initial summary in question. In case of inconstancies the above summarizing statements shall prevail and bind us accordingly.

II. 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, please contact our data protection team by email: dataprotection@vereign.com.
III. LEGAL FRAMEWORK

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 explicitly explain to you the exact purpose of the concerned data processing and you may at any time retrieve your consent given to us.

IV. 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. PROVIDING YOU WITH A NEXT GENERATION REGISTERED EMAIL

In order to provide you and your recipients with a tamper-proof verification and evidence of your sent email just as well as a respective revision-secure archiving, we process data related to your emails and attachments (hereinafter collectively: Email Data) locally on your device. Overall the purpose of this data processing is to provide an independent and self-sovereign proof for your email and attachments, way beyond what traditional solutions like handwritten signatures or registered mail services could offer.

a) OVERALL PRIVACY BY DESIGN CONCEPT

In order to protect your Email Data we have implemented a strong form of pseudonymization, which is the foundation of our privacy by design concept. Before any of your Email Data is leaving your device (e.g. your laptop or mobile phone), for the purpose of providing your with the Vereign Services, your Email Data is compressed, encrypted (AES-256 GCM) and subsequently shredded in random data pieces (this entire process is hereinafter referenced as “SEALing”). One part of this shredded data (together with one-time encryption keys) is exclusively stored in a QR code which is attached to the email body of the user (we call this QR code “QR SEAL”). The other remaining part of the shredded data goes a separate way and is stored on remote servers (we call this part of the data “QR TAIL”). None of these two random data pieces alone can be restored into your original Email Data. Only in case the private QR SEAL is present it will be technical feasible to identify the matching public QR TAIL and combine both data pieces in order to restore and authenticate your Email Data (hereinafter referenced as “deSEALing”).

Overall, this means it will only be feasible for us (or anyone else) to conduct a deSEALing process with the help of the public QR TAIL, in case the matching QR SEAL is present - which by itself is part of your email, already containing all the data elements that can be revealed by joining the QR SEAL with the QR TAIL.

b) SEALing of your email and attachments

In the following we will explain what happens with your personal data in detail, in case you choose to send an email with one of our Vereign Applications activated.
aa) Metadata
Comparable to a receipt, evidencing your email and attachments have been send at a certain point in time, and in order to offer a respective tamper-proof and automatically (if required also manually) verifiable audit-trail, the following metadata will be collected locally on your device:
- 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”)
This Metadata undergoes the already explained process of SEALing, locally on your device. The resulting QR SEAL is attached to your email and your public QR TAIL is send of to be stored in a resilient cloud environment.

bb) Hashes
In order to provide an additional layer of independent and tamper-proof evidence, we are writing hashes to a public Blockchain. Hash functions are widely used to mathematically prove 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 again locally on your device 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 your QR TAIL. These hashes in your QR TAIL are secured by your QR SEAL, meaning without having access to your QR SEAL, nobody has access to the hash and to its confirmational value in regards to your Sender Input Data.
We are writing hashes of the already hashed QR TAIL to a public Blockchain network administrated by Æternity Establishment.
Given their complexity, for the hashes in the QR TAIL but even more so for the resulting double hashed Blockchain entries, it is technically possible to brute force and invert them, without having access to your Sender Input Data anyway.

c) Archive for email and attachments
Comparable to a revision secure archive, we make it possible to download the authenticated and validated email including its attachments (if any). The process of SEALing and deSEALing of the content of your email and attachments is once again as described above. So again, the QR SEAL acts as a key that is able to access and decrypt the missing (by itself abstract) data of the public QR TAIL. You email and attachments will only be accessible for somebody, already having access to your QR SEAL and again the deSEALing process happens locally on the device of the individual user.
Due to the fact that our mission statement is to provide you with a self-sovereign and tamper-proof solution, we are storing the public QR TAIL in the Interplanetary File System (IPFS), for more information on this truly remarkable technology see https://ipfs.io/. We are hosting our respective IPFS nodes in our professional data center in Switzerland. Such an IPFS Storage offers you (and your recipients) the unique opportunity to also pin your public QR TAIL or instruct any other service provider to pin this public data for you. This way, you may choose to become truly the sovereign of your evidential data, that is connected with your QR TAIL.
c) deSEALing of your email and attachments

aa) deSEALing and verifying your Email Data with Vereign Applications

With the help of our Vereign Applications you are able to securely conduct the process of deSEALing and join the private QR SEAL with the public QR TAIL, locally on your device. The public QR TAIL is requested by your device and the private QR SEAL does not leave your device. This even applies in case you simply click or scan the QR SEAL and a web application is started in your browser.

bb) Providing a Reciever audit-log

In case you installed one of our Seal Application on your device and use it for an automatic deSEALing and respective verification of emails send by another user of our Vereign Services, the sender will receive an automatic acknowledgement of receipt, as soon as the mail as been authenticated.

This does not apply in case you (or your receiver) is merely clicking or scanning a QR SEAL and accessing the web verification app. Our web verification app does not send such automatic acknowledgement of receipt.

Basically, this auto acknowledge function is comparable to what 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 recipient email address

(herinafter "Recipient Input Data")

This hash of Recipient Input Data is encrypted with the one time public key of the sender and stored again in in a resilient cloud environment and finally as a doubled hash on a public blockchain, just as pseudonymous and obfuscated as described above.

2. SUBSCRIPTION AND CUSTOMER FEEDBACK DATA

In case you are subscribing to our Vereign Services as a customer, there is some other data not related to your individual emails and attachments, we need to process. Such data includes your email address you have provided during the subscription onboarding and related information, like when did your subscription start and when your free trail (or already paid subscription period) will end. We store and process such information, solely for the purpose to administrate your subscription and customer relationship. Therefore we may also use your contact details occasionally to keep you informed about new aspects of our Vereign Services and our software development. Also we may ask about your user experience and other relevant feedback.

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.

3. PAYMENT DATA

Your credit card number and payment related information is especially sensitive. Therefore the Payment Card Industry Data Security Standard ("PCI DSS") defines a set of security standards to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.
In order to provide you with a such a secure, PCI DSS compliant, payment option for your Vereign Service subscription, we are using Stripe Inc., as a payment gateway provider. As soon as you are choosing to provide us with your payment details in the billing section of your Vereign Service subscription, Stripe Inc. is using cookies for the purposes of user authentication, fraud detection, fraud prevention. A full disclosure of Stripe Inc. use of cookies, including persistent cookies, is documented online at https://stripe.com/cookies-policy/legal. Placing these Stripe cookies and the subsequent data processing by Stripe Inc. is an essential part of a secure and compliant payment operation and we cannot offer any service that depends on your payments if these cookies are disabled.

V. DATA ERASURE AND STORAGE PERIOD

In summary we keep your public QR TAIL for 10 years and your subscription data as long as you are subscripting to our Vereign Services.

1) PRIVATE QR SEAL

As explained above your private QR SEAL is exclusively 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 to erase these emails from the respective email accounts (or any backups you or your recipients may have created). But naturally, you may at any point in time arrange for the deletion of any of the distributed copies of the QR SEAL with your chosen recipients. As soon as you accomplish such a complete deletion of the distributed QR SEAL, all data connected with your public QR TAIL will be barred from access permanently. But we have no way of identifying the recipients you sent the QR SEAL to, hence we cannot offer you any assistance for erasing your distributed QR SEAL.

2) PUBLIC QR TAIL

We will keep the QR TAIL which contains the pseudonymous, encrypted and shredded data, related to your Metadata in a resilient cloud storage for a period of 10 years (erase process will be done once a year at the end of a calendar year). Same applies for pseudonymous, encrypted and shredded data in the QR TAIL, related to the content of your email and attachments, which we make available for you and any of your recipients in our IPFS node.

As long as a copy of your private QR SEAL (which is part of your sent email) exists, the stored public QR TAIL will help to restore your Metadata and content of your email and attachments, and thereby provide reliable evidence that your email and attachments are authentic, have been sent at given point in time and have not been altered. But by itself your public QR TAIL is just a seemingly random sequence of characters discoverable by an abstract one time identifier. That means, after all copies of your QR SEAL have been erased, the QR TAIL will have no counterpart and will consequently bear no significance whatsoever. Also that means, by itself the QR TAIL is entirely pseudonymous, and the only way to get something meaningful out of it, is to combine it with your private QR SEAL. In particular, even we cannot even identify the abstract QR TAIL that have been created for you, without you providing us with the matching QR SEAL.

But please note, in case you have chosen to share your email (including your QR SEAL) with other recipients, these recipients will be technically able to join the individual QR SEAL with the corresponding QR TAIL and thereby may access the conformational value of the QR TAIL.

Same applies, in case your recipients share the QR SEAL 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 exclusively a matter between you and your recipients. In particular please also note, anyone having access to your email (legitimately or illegitimately) will already have access to all of your actual personal data and information that are contained in the QR TAIL.
Last but not least, please also understand that as explained above, we offer the public QR TAIL in our IPFS node, to be pinned by you or your recipients. Hence you or you recipients may decide to store the public QR Code dependently from us. Please note that this outcome one of the very reasons to use our Vereign Application, the purpose here is to provide you and your recipients with extremely reliable and self-sovereign proof and trust – independently from certain service providers, which includes us.

3) HASHES ON THE BLOCKCHAIN

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 all copies of the QR SEAL or the corresponding QR TAIL is erased.

As long as a copy of your sent email (including the QR SEAL) exists, the hashes on the public Blockchain will provide an additional layer of reliable evidence that your Sender Input Data and your Recipient Input Data is authentic and has not been altered. But by itself the 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 QR SEAL or the QR TAIL have been erased, the abstract hashes 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 hashes, leaving the abstract hashes without relevance for you and any of your personal information.

4) PAYMENT AND SUBSCRIPTION DATA

As explained in clause IV, 4 “Secure Payment Gateway”, we are not processing your actually sensitive payment data, like your credit card number. But we do need to store and process you contact details and the details of your Vereign Service subscription, as long as we have a legal reason to do so according to our contractual relationship. After this legal reason has expired (in particular after you cancel your subscription), we will erase this data.

VI. 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.

However, for specific tasks, like storing your QR TAIL in an resilient and secure 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 bound by confidentially, this privacy policy and any applicable law, including but not limited to GDPR.

VII. YOUR RIGHTS AS A 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.

VIII. 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. At Vereign we seek to combine and align our overall requirements concerning cyber security and resilience, regardless whether these requirements are derived from best practise approaches, applicable law or contractual regulations. This holistic point of view makes it feasible for us to deal with the respective requirements in a transparent and effective way. As part of our security management processes,
we obligated ourself to conduct regular external penetration tests of our Seal Applications and its underlying processes.

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 cannot provide any guarantee that access to your data by third parties is averted.

**IX. 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. Therefore this Privacy Policy may be amended from time to time, provided that nothing in newer versions of this Privacy Policy shall contradict the summary given to you in clause 1 above ("overview about our commitments").

As of: February 2022