GENERAL DATA PROTECTION REGULATION

KeeeX takes every precaution to maintain the security and confidentiality of all processed personal Data. Our goal is to prevent such Data from being modified, damaged, shared or accessed by unauthorized third parties.

PREAMBLE ON PERSONAL DATA AND THE GENERAL DATA PROTECTION REGULATION (GDPR)

The EU's General Data Protection Regulations have been in place since 2018 May the 25th and aims to strengthen the protection of the personal data of EU citizens. KeeeX obeys the spirit and the letter of the GDPR. In particular:

- **KeeeX does not trade your data, metadata or activity trails or use such data to train machine learning systems or artificial intelligences.**
- **In the vast majority of cases, KeeeX's web services do not see your data, do not see your metadata and cannot trace your activity, because everything takes place on your own devices (applications, on premises services or mobile apps).**
- **KeeeX takes only the bare minimum amount of data required for your use of software and services: name, first name and email if required, and offers anonymous or pseudonymous services when possible using freely selected digital identities under the sole control of users.**
- **KeeeX encrypts all direct end-to-end exchanges between users with secrets under their sole control, and encrypts all software connections between them and web services using encrypted connections under TLS/SSL.**
- **KeeeX keeps no record of your activity other than strictly necessary for the operation of software and services, and destroys any notification or data encrypted within a maximum of three months.**

For further details, please feel free to write to dpo@keeex.net. We maintain summary documents including a personal data registry and our risk management procedures.

Note that KeeeX will never ask for unwanted or unrequired sensitive personal data.

We maintain summary documents including a registry of processing activities relating to personal data and a document concerning our risk management procedures.

In almost all cases, personal data will be retained solely for the time required to provide the customer with the desired services.

USE OF DATA BY KEEEX AND USE OF PERSONAL DATA

The KeeeX technology ensures, barring a specific request or solution accepted in writing by KeeeX and the user, that user data remain exclusively on their devices and under their total control. KeeeX has no possibility of exploiting this data, particularly through AI or Data Mining tools, or to derive user profiles for commercial purposes.

In all cases, KeeeX offers collaboration services that provide ultimate confidentiality during exchanges, including:

- **The systematic use of TLS/SSL encrypted connections to KeeeX's servers with Let's Encrypt (or other) certificates, including extended-validation certificates when requested.**
- **end-to-end encryption of user-to-user data (KeeeX engineers have no way to access encrypted content except when explicitly intended for it).**
- **the obfuscation of encrypted data (lack of information to infer the nature, the issuer, the recipients of an encrypted data blob).**
- **the user's free choice of the transport channel of his data, especially via means of synchronization under his control (private cloud, corporate network drive ...).**
- **Digital signature by means under the exclusive control of the user (private keys and/or Fido keys orothers).**

In order to provide the Service, KeeeX web services may use the following Metadata: idx (file print, transmitted only for time stamping) and idr (user profile print, transmitted for notifications). These cryptographic fingerprints are said to be non-reversible: i.e. they never allow for making any assumptions about the content they represent.

For the purpose of ensuring the operation of the services, KeeeX does not transfer any clear or reversible data if this is not strictly required technically.

Except when required by law, KeeeX does not retain any user data beyond the requirements for their technical use and the provision of a quality user experience. To date, notifications and encrypted data are not kept for more than three months.

You understand and accept that the use of validation, publication or revocation of digital identity or blockchain anchoring services with information intended to be incorporated into publicly auditable online registries involves a public release of the following non-inversible data: fingerprints of documents, cryptographic public keys and associated signatures, and any other data you may have included.

You also understand that data on a public blockchain cannot be erased or changed.

The personal data collected by KeeeX is processed by computer to manage your KeeeX account and the rights attached to it. To date, KeeeX retains only the names, first names, emails and traces of its users' passwords. Passwords are never received by KeeeX's servers

other than in the form of non-reversible derivations and carried out in such a way as to make so-called "dictionary" attacks very difficult.

In order to improve the Service and allow for pay-as-you-go billing, you agree with KeeeX's collection and use of Service usage statistics, including the number of files processed, transmitted, signed, verified, time-stamped. These statistics are not associated with any information other than your user profile and/or company.

IN CASE OF DATA BREACH

KeeeX implements several security measures. However, we anticipate all scenarios, including those that include an information breach.

In this event, we undertake to inform affected customers as soon as possible. This notification will specify the nature of the incident, its foreseeable consequences, and the steps taken to resolve or minimize the breach.

SECURE DATA STORAGE SYSTEM

Unless expressly requested by a customer, storage is done in Data Centers located in Europe, mainly in France, with two providers: OVH and Amazon Web Services. The contracts that bind us guarantee the maintenance of data in Europe.

Access to the storage service of our providers is strictly limited to KeeeX and secured by several authentication systems, including Fido, Yubikey and SSH.

The data in transit is encrypted via TLS which allows security of exchanges between KeeeX and the services of its providers.

KeeeX takes care to inquire and verify that these two providers OVH and AWS are also vigilant in complying with the data protection guidelines wrt. their customers, whether regarding physical or digital Data.

REGISTRY OF THE PROCESSING OF PERSONAL DATA

For all of our software and applications, we have a registry of processing activities to compile a complete inventory of the types of data processing carried out, the type of data needed for these treatments, their lifecycle and the people and recipients involved.

This registry is updated in real time and is regularly monitored.

USE OF SUBCONTRACTORS

With the exception of the subcontracting companies that we officially use, no other company is able to view or access our customers' personal data.

However, in the event that KeeeX were to outsource activities involving visualization or access to data by a new subcontractor in the future, this change would be subject to an agreement of our customers.

All of our subcontractors are located on European territory and are therefore subject to the commitments enforced by the European General Data Protection Regulation.

We maintain an exhaustive list for all of our subcontractors, and are assured that all those who deal with personal data undertake to comply with existing legal frameworks.

This list is updated in real time and is regularly checked.

COOKIE MANAGEMENT

Cookies used on our site and our applications do not collect any personal data and are simply used for authentication and as a login witness.

APPOINTMENT OF A DATA PROTECTION DELEGATE (DPD)

We have appointed a DPD to monitor compliance with the RGPD within the company. He is also the preferred contact for our customers for any information related to data protection.

In accordance with the "Computer and Freedoms" Act of 6 January 1978 and the European Parliament's 2016/679 Regulation (EU) and the Council on the Protection of Individuals with respect to the processing of personal data and the free movement of such data, you have the right to access and correct information about you.

Contact our DPD: dpo@keeex.net..

KEEEX'S COMMITMENTS AS A SUBCONTRACTOR

KeeeX is committed to implementing the following actions:

- **process personal data for the sole purpose of performing services: KeeeX will never process your information for other purposes (marketing, etc.).**
- **don't trade your data.**
- **do not transfer your data outside the European Union.**
- **inform you of any use of subcontractors who may process your personal data.**

- **to implement high safety standards to provide a high level of security for our services.**
- **notify you as soon as possible in the event of a data breach.**

Thanks for using KeeeX!