

# Privacy policy

**Platform of Trust Oy's SignSpace user register and signing event register**  
(Last updated on 10 February 2021)

## 1. Controller

Platform of Trust Oy, Business ID 2980005-2  
Tarvonsalmenkatu 17 B  
02600 Espoo  
Finland

Data Protection Officer's contact information:

Email: dpo@vastuugroup.fi  
Mail: Platform of Trust Oy  
c/o Vastuu Group Oy  
Data Protection Officer  
Tarvonsalmenkatu 17 B  
02600 Espoo  
Finland

## 2. Data subjects

Data subjects are users of SignSpace service.

## 3. Purposes of processing

Personal data is processed for the following purposes:

- providing SignSpace service
- maintenance, support and further development of the service
- witnessing validity of the electronic signatures made within the service
- customer service and management of customer relationship
- service invoicing
- risk management and ensuring data security of the service
- prevention and investigation of misuse of the service
- marketing of controller's and its business partner's other services that are targeted mainly to businesses

## 4. Data content

Data file contains the following data provided by the registered user by him/herself during the registration:

- name
- person ID
- user credentials
- email, phone number and other contact information provided by the user
- profile picture

During the use of the service following data may be collected:

- technical user identifiers
- account registration date
- status of the account
- time and manner how the user was identified in the service
- user's full name provided at the time of identification

- information on user's personal certificate and its validity
- information of the acceptance of terms of service
- organisation account(s) for which the user is linked to
- start date and end date of rights to use any organisation account
- log data on the activities user has taken in the service

In connection with a signing event the following data may be collected:

- time and manner how the user was identified in connection with the signing event
- any data on user's authority to sign on behalf of the organisation account
- time of signature
- device used for signing, IP address, other data collected to signing log files
- electronic seal that can be used to verify that the signed document has not been tampered after the signing

## **5. Regular data sources**

Registered users are identified in the service using controller's and its business partners' electronic identification methods such as bank ID or mobile certificates.

Personal data is gathered mainly from the registered person or from the organisation on behalf of which the user uses the service.

## **6. Regular disclosure of personal data**

In general, Controller will not regularly disclose user register data to any third parties.

During use of the service user's name, email, profile picture and represented organisation account will be disclosed to other users that are participating discussions in the same group (space or thread).

Personal data concerning a signing event and written on the electronically signed document may be disclosed in electronic format to all users and organisations that were granted access to the same group (space or thread).

Controller may disclose to a third party information from the signing event register if a presented signed document is unmodified.

Controller may disclose evidence on the validity of a signature on request of a party who is relying on validity of the signature or on request of a competent authority.

In the production of the service, Controller can use subcontractors located within the European Economic Area, and it can also transfer personal data to such subcontractors for producing the service

## **7. Duration of processing activities**

Controller will retain personal data stored in the user register and signing event register as long as such data is needed for the purposes of providing SignSpace service to its customers. However, data stored in a signing event register will be stored at least 10 years from the end of the calendar year during which the document was signed.

## **8. Transfer of data outside the EU or EEA**

Customer's Content and personal data included in such Content will not be transferred outside the European Economic Area (EEA).

Personal data concerning users is not principally conveyed outside the EEA, unless necessary for the technical implementation of data processing, e.g. when the data subject sends or receives messages by email or other online-based transmission service.

Controller may use in its service related support functions such as in customer communications, Customer Service ticket management and in automated error log processing third-party data systems

and cloud services, the personal data processing of which can be partly implemented outside the EEA. To the extent that Controller's subcontractors implement data processing outside the EEA, Controller will ensure that the amount of the personal data to be transferred is minimized to what is necessary for the purpose and that the transfer of personal data outside the EEA is completed in accordance with the applicable legislation.

## **9. Data security**

The right to use the register is restricted to appointed persons only, who need the information concerned in their work tasks. Each user has his/her own user name and password. Personal data is stored in databases and data systems located within the European Economic Area that have the appropriate technical and organisational measures in place to protect the personal data against misuse and disclosure.

## **10. Rights of data subjects**

As a data subject, you have the right to inspect the personal data concerning yourself and demand that any incorrect data be corrected or deleted. However, we can, within the limits of law, restrict your right to access data that contains the personal data of others, is a business secret of ours or our customer, or is related to the safety features of the service.

You have the right to request that your personal data be deleted in situations specified in the general data protection regulation, if:

- you cancel your previous consent and there is no other legal basis for processing the data concerned besides your consent
- you object to the processing of your personal data, and there is no legal basis for continuing the processing
- processing the data is illegal
- you are under 18 and your personal data was collected in connection with providing information society services.

In situations specified in the general data protection regulation, you have the right to object to the processing of your data or to request that the processing of your data is restricted. If you consider the processing of your personal data to be illegal, you can submit a complaint on the processing to a competent authority.

## **11. Contacts**

If you have questions regarding this privacy statement or you wish to exercise your rights, please contact Controller's data protection officer by using the above email or postal address.

## **12. Changes**

Controller can make changes to this privacy statement from time to time without a separate notice. Any changes made are listed in the "last update" section at the beginning of this privacy notice.