Accessibility and personal data

You have access to your basic personal data (mainly your name and email address) through your account on the Agrello Platform. This access is secured with your Agrello ID digital private KEY and PIN codes. Keeping your Agrello ID digital keys secure and keeping your PIN codes a secret ensures the safety of your personal data.

Any biometric data obtained as part of the identity verification process is processed and stored securely by our trusted identity verification partner. They meet the industry level of privacy and security for the data.

Agrello Platform has access to your basic personal data (mainly your name and email address) using internal access credentials over a secure channel. This access is used by the Agrello Platform to let you manage your account and to populate your details in your contracts.

We do not share or sell your personal data. Your basic personal data (mainly your name and email address) is stored in a secure database.

Validity of signed documents

Agrello uses industry-standard ASIC (Associated Signature Container) format for archiving, storing and timestamping documents along with associated signatures. They can, therefore, be validated using any compatible publicly available tools such as DigiDoc or Nowino web solution.

Signed documents and files you upload onto the Agrello Platform are stored in industry-standard ASIC containers in a secure Agrello database.

Blockchain technology

Agrello creates a link between your public keys and your verification session ID and saves that link in your digital identity on the Agrello blockchain as an immutable reference.

Upon signing, a signature transaction is posted from your Agrello digital identity to the Agrello blockchain (verifiable in the Agrello Blockchain Explorer), linking your digital identity public key, the hash of the signed document(s) and the actual fact of signing.