intertrust®

The Intertrust Platform™

Data privacy and security fact sheet

The Intertrust Platform™ is a secure data rights management platform purpose-built for enabling secure collaboration on proprietary data. The Platform is designed to address many complex and sensitive big data privacy scenarios. This overview summarizes how the Intertrust Platform ensures data protection and privacy.

Identity and access management

The Intertrust Platform supports multiple ID providers, with a built-in solution that supports industry standard authentication, including MFA, and identity federation protocols such as OpenID Connect and OAuth2.

All access to APIs and user interfaces require an access token to be present. The access token is validated for every request and must be acquired via Intertrust Platform authentication service. The service provides various methods for authentication, such as OAuth2 and OpenID Connect. Third-party IdPs, SAML, LDAP are in development.

In addition to this, multi-factor authentication can be required as well. The supported types are TOTP and SMS.

The access control service allows the user to specify granular permissions that are enforced across all interfaces by the central authorization service.

All authorization events are logged as immutable event records for auditing and compliance purposes.

Data security

Intertrust Secure Execution Environments provide configurable networking and governance options. This allows computational workloads to be run within an isolated, auditable, access-controlled environment, thereby reducing the risk of unauthorized access and irrevocable data duplication.

The audit logging services collect immutable audit logs for all operations executed in the platform on behalf of a user, which enables the tracking and auditing of all accesses to customer data.

Customers have full control over data governed by their Intertrust Platform deployments, including data stored in the Intertrust Time Series Database and datasets derived from virtualized data sources, such as external databases.

Intertrust does not access any customer data for any purpose without customer consent. Usage logs are kept on all data access events. The company transfers data hosted within the Intertrust Time Series Database to other regions only as specified by the customer controlling the data.

Storage

Intertrust operates instances of its secure data processing platform in various regions of the world including the EU. There are regional teams operating these instances, enabling full control over cross-border data transfers.

Intertrust conducts regular penetration testing to keep Intertrust Platform security level up to date.

The Intertrust Platform separates and abstracts storage, index, and query into a virtual database system with integrated access control.

The Intertrust Platform's architecture is modular, extensible, and may be adapted as needed, allowing storing data in different locations and formats.

Data subject requests

Intertrust supports Data Subject Requests for the GDPR and CCPA (California Consumer Privacy Act).

Data classification

Intertrust has adopted a Data Classification and Handling Policy.

Any data that is protected by laws or regulations, including privacy laws and regulations, and data protected by confidentiality agreements, is classified as confidential data.

Anonymization

The Intertrust Platform allows anonymization of any identifiable information managed by its users, enabling GDPR compliance even if operating with sensitive Personally Identifiable Information (PII).

Privacy by design

Intertrust has implemented a Privacy by Design process. All Intertrust Platform development work is being reviewed at the design and later stages of the product development life cycle and will only be launched if all applicable privacy requirements are met.

Data breaches

Intertrust has adopted a Breach Notification Policy and assigned a Breach Notification Team.

Any security incident discovered by an Intertrust employee and involving personal data has to be reported within four (4) hours of identifying a potential incident.

A reportable breach determination must be made within 48 hours of the initial notification and Intertrust will report it no later than 72 hours after becoming aware of the incident.

Legal compliance

Intertrust offers customers a Data Protection Addendum and EU Standard Contractual Clauses that are compliant with GDPR.

Intertrust has appointed a Data Protection Officer who oversees compliance with the GDPR.

intertrust®

Building trust for
the connected world.

Learn more at: intertrust.com/platform
Contact us at: +1 408 616 1600 | dataplatform@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035