SECURITY AND PRIVACY DOCUMENTATION

CERBOS HUB

Updated: 23 November 2023

Cerbos has implemented the following technical and organisational security measures to provide the ongoing confidentiality, integrity, availability and resilience of processing systems and services for Subscription Services branded as Cerbos Hub (the "**Covered Services**"), including protection of Customer Data as defined in the Cerbos Data Processing Addendum available at https://legal.cerbos.dev/agreements:

1. Confidentiality

Cerbos has implemented the following technical and organisational security measures to protect the confidentiality of Covered Services, in particular:

- Cerbos processes all Customer Data on remote server sites owned and operated by industry leading cloud service providers that offer highly sophisticated measures to protect against unauthorised persons gaining access to data processing equipment.

- Cerbos implements suitable measures to prevent its data processing systems from being used by unauthorised persons. This is accomplished by:
    - automatic time-out of user terminal if left idle, identification and password required to reopen
    - issuing and safeguarding identification codes;
    - letting customers define individual user accounts with permissions across Covered Services.
- Cerbos's employees entitled to use its data processing systems are only able to access Customer Data within the scope of and to the extent covered by their respective access permission (authorization). In particular, access rights and levels are based on employee job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. This is accomplished by:
    - limited access to Customer Data to only authorised persons;
    - industry standard encryption.

2. Integrity

Cerbos has implemented the following technical and organisational security measures to protect the integrity of processing Covered Services, in particular:

- Cerbos implements suitable measures to prevent Customer Data from being read, copied, altered or deleted by unauthorised parties. This is accomplished by:
    - performing annual penetration tests of Cerbos Platform;
    - following a secure development policy of Cerbos Platform;

- Cerbos implements suitable measures to prevent Customer Data from being read, copied, altered or deleted by unauthorised parties during the transmission thereof or during the transport of the data media. This is accomplished by:
    - use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;

- industry standard encryption; and
- avoiding the storage of Customer Data on portable storage media for transportation purposes and on company issued laptops or other mobile devices.

3. Availability

Cerbos has implemented the following technical and organisational security measures to protect the availability of Covered Services, in particular:

- Cerbos designed suitable measures to provide that Customer Data is protected from accidental destruction or loss. This is accomplished by:
  - infrastructure redundancy;
  - policies prohibiting permanent local (work station) storage of Customer Data; and
  - performing regular data back-ups.

4. Resilience

Cerbos has implemented the following technical and organisational security measures to protect the resilience of Covered Services, in particular:

- Cerbos designs the components of its platform to be resilient by selecting the best-in-class infrastructure providers with data centres that have daily backups with high uptime and availability.

Return of Customer Data

Within thirty (30) days post contract termination, Customer is able to extract Customer Data submitted to the Covered Services (to the extent such data has not been deleted by Customer) through either export via built in reports or via API. For selected Services, Customer can choose to purchase a read only subscription allowing for data to be retained within the system for as long as required by Customer.

If the reports or API is not available for the applicable Service and within thirty (30) days post contract termination, Customer can request the return of the Customer Data submitted to the Covered Services (to the extent such data has not been deleted by Customer) that will be provided by Cerbos to Customer in a commonly-used machine-readable format.

Deletion of Customer Data

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for thirty (30) days, after which it is securely overwritten or deleted from production within sixty (60) days. The Customer Data can be retained as part of the regular database backups for up to ten (10) years and cannot be deleted individually. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request the return of their Customer Data submitted to the Covered Services, Cerbos reserves the right to reduce the number of days it retains such data after contract termination. Cerbos will update this Security and Privacy Documentation in the event of such a change.

Processing of User Account Data

To create and administer user accounts and access the Covered Services, customers must provide information about users ("**User Account Data**"). User Account Data includes information such as name, username, business address, job title, country/region, phone number, and email. Cerbos processes User Account Data to provide its customers with the Covered Services; in that case, personal data about users is treated as Customer Data. Cerbos also processes User Account Data for certain of its own business purposes, such as account administration, invoicing, and licensing compliance, and treats it consistently with the Cerbos Privacy Statement.