



## SECURITY AND PRIVACY DOCUMENTATION

### PROFESSIONAL SERVICES

**Updated:** 23 November 2023

Cerbo has implemented the following technical and organisational security measures to provide the ongoing confidentiality, integrity, availability and resilience of its workstations and other systems to protect Professional Services Data during the provision of the Professional Services (the “**Covered Services**”):

#### 1. Confidentiality

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

- **Limited access.** The Covered Services are operated in a manner designed to segregate and restrict Professional Services Data access based on business needs. Our processes provide logical data separation for different customers and, depending on the Covered Services, may allow the use of customer and user role-based access privileges.
- **Workstations.** All Cerbo workstations (which, as used herein, refer to laptop and desktop computers provided by Cerbo to its personnel) that are used to process Professional Services Data in the course of the provision of Professional Services (each a “Workstation”), are protected by measures to ensure the confidentiality and integrity of such information, including the following:
  - Application and operating system patches and services packs are kept up-to-date.
  - A real-time virus scanner is installed and running; signature files are kept up-to-date; the virus scanner runs a daily scan of the Workstation.
  - An anti-spyware solution is active; signature files are kept up-to-date; anti-spyware scans are run at least weekly.
  - Workstations used for the performance of Professional Services have full disk encryption using the Advanced Encryption Standard (AES) with a minimum key length of 128 bits.
  - Access to a Cerbo Workstation requires the user to enter their unique user ID and password. All Cerbo users are required to keep and maintain complex passwords.
  - User access to the Cerbo corporate network requires multi-factor authentication.
  - Cerbo has and shall maintain policies that prohibit the use of personally-owned workstations for the processing of Professional Services Data by Cerbo employees.
  - Workstations are documented and tracked in a formal asset management system.
- **Security Policies.** Professional Services are provided in accordance with the following policies and procedures to enhance security:
  - Cerbo users are required to change their passwords at regular intervals, and may not use the three most recently used passwords.
  - Cerbo users are required to maintain uniquely identifiable user IDs to ensure accountability for all activities, actions, and access to Professional Services Data.
  - Cerbo limits its use of Professional Services Data it receives when providing Professional Services to that appropriate to providing its services to Customer.

- Cerbos personnel who have access to Professional Services Data are informed of the confidential nature of the Professional Services Data through appropriate training on their responsibilities with respect to access to such types of information.
- All Cerbos employees providing Professional Services must complete annual mandatory security and privacy training. Completion is tracked by Cerbos.
- **Incident Management.** Cerbos maintains security incident management policies and procedures. Cerbos notifies impacted customers without undue delay of any unauthorised disclosure of their respective Professional Services Data by Cerbos or its Sub-processors of which Cerbos becomes aware, to the extent permitted by law.

## 2. Integrity

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

- **Logs.** Cerbos has and shall maintain system event logging procedures for Workstations and Cerbos internal network systems that access or store Professional Services Data, namely: (a) event logs for all security devices, perimeter devices, and policy enforcement points (including firewalls, VPN servers, and intrusion detection systems); (b) network log-on records from authentications systems, including domain controller logs.

## 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 Professional Services Data is protected from accidental destruction or loss. This is accomplished by:
  - Utilizing tools with infrastructure redundancy; and
  - Policies prohibiting permanent local (work station) storage of Professional Services Data.

## 4. Resilience

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

- Cerbos incorporates resilience into its Professional Service operations by selecting the best-in-class tools with regular backups, high uptime and availability.

### **Return and Deletion of Professional Services Data**

Cerbos has implemented policies and procedures designed to ensure that Professional Services Data will not be stored on Workstations or other physical media provided by Cerbos and used to perform Professional Services, unless necessary to provide Professional Services.

Excluding any Professional Services Data that may have been, at Customer's instruction, submitted to the Subscription Services and that is now Customer Data as defined in the MSA, upon request by Customer after the effective date of termination or expiration of the relevant Order Form (the "Expiration Date"), Cerbos will make the Professional Services Data in its possession or control available to Customer, to the extent applicable, for return, export or download for a period of 30 days after the Expiration Date. Cerbos will otherwise have no obligation to maintain any Professional Services Data. Please note that Cerbos may not always know whether Customer wishes to have its data deleted after termination or retained for use in a future Professional Services engagement. If Customer does not expect to ask Cerbos to Process its Professional Services Data further, it should inform Cerbos, and at the Customer's instruction Cerbos will delete Professional Services Data in its possession or control, unless legally prohibited.

### **Sensitive Data**

Important: If Customer chooses to provide sensitive or regulated data, then Customer is responsible for ensuring compliance with all applicable laws and regulations. Cerbos makes no representation that its Professional Services are compliant with laws related to sensitive or specially regulated data, including without limitation government-issued identification numbers; financial information (such as credit or debit card numbers, bank

account numbers, and any related security codes or passwords); personal health information; or other data subject to special legal requirements.

For clarity, the foregoing restrictions do not apply to financial information provided to Cerbos for the purposes of checking the financial qualifications of, and collecting payments from its customers, the processing of which is governed by Cerbos' Privacy Statement.

**Third-party tools**

In the performance of Professional Services, Cerbos may use other third-party tools at Customer's instruction or with Customer's consent, including as referred to in the applicable Order Form(s), or tools that do not qualify as Sub-processors (e.g., tools that are entirely on-premise or cloud tools that do not Process Personal Data).