Celonis Information Security Annex

This Celonis Information Security Annex (the "Annex") sets forth the IT security and controls applicable to Celonis' provision of EMS (defined below) and is incorporated into and made part of Your agreement (including any Orders) governing Our provision of EMS to You (collectively, the "Agreement").

1. **Definitions.** All capitalized terms in this Annex have the meanings specified in the Agreement, except as otherwise provided below:

1.1 **"EMS"** means the Celonis Execution Management System, as made available to You under the Agreement.

1.2 **"High Availability"** means the elimination of single points of failure to enable applications to continue to operate even if one of the underlying IT components fails.

1.3 **"Information Security Incident"** means any confirmed (i) unauthorized access to, alteration of or damage to the EMS, or (ii) loss or unauthorized alteration of or damage to Customer Data or (iii) theft or unauthorized use, disclosure or acquisition of or access to any Customer Data.

1.4 **"Malware"** means any program or device (including any software, code or file) which is intended to prevent, impair or otherwise adversely affect the access to or operation, reliability or user experience of any computer software, hardware or network, telecommunications service, equipment or network or any other service or device, including without limitation worms, trojan horses, viruses, ransomware, trap doors and other similar malicious devices.

1.5 **"Principle of Least Privilege"** means allowing access for users (or processes acting on behalf of users) only as necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

2. **Our Obligations.**

2.1 We will comply with, and will cause Our employees to comply with, this Annex. As between You and Celonis, We are responsible for any failure of Our subcontractors to comply with any IT controls set forth in this Annex.

2.2 We will maintain Our comprehensive information security program in compliance with industry-recognized standards and applicable law. Our information security program includes administrative, technical, physical, organizational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Customer Data, and (ii) mitigate the threat of Information Security Incidents. Our information security program also includes a cybersecurity awareness program that informs and reminds employees of preventative measures to avoid inadvertent exposure of Customer Data or inadvertent exposure of EMS to unauthorized activity.

2.3 We will regularly test, review and update Our information security program.

3. **Standards / Certifications.**

3.1 We will maintain, and will provide to You upon request and subject to confidentiality requirements, any then-available proof of attestations of compliance with certifications and standards which may include, without limitation, the following:

i. SOC 1, Type 2;
ii. SOC2, Type 2;
iii. ISO 27001:2013;
iv. ISO 27701:2019;
v. TISAX; and
vi. ISO 9001:2015

3.2 You may view Our current list of certifications and compliance status at http://trust.celonis.com/.

4. **Encryption.**

4.1 We will provide encryption for Your connection to EMS with a minimum encryption level equivalent to AES-128 (or then-current industry equivalent).

4.2 We will encrypt all Customer Data residing on backups with a minimum encryption level equivalent to AES-256.

4.3 We will encrypt Customer Data at rest with a minimum AES-256 bit encryption. Data will be encrypted, whether the storage device is powered on or off.

4.4 We will store secrets (i.e. encryption keys, certificates, passwords, hashes) in an appropriate service. We will not store system secrets in configuration files or in source code and will implement access controls designed to ensure that access to such information follows the Principle of Least Privilege.

4.5 We will encrypt all passwords with a minimum encryption level equivalent to AES-256

4.6 If You have purchased a private cloud instance, We will support use of encryption keys supplied by You (bring or hold Your own encryption key) and will provide a means of allowing You to rotate the key as documented in Our then-current product documentation.

5. Controls.

5.1 EMS.

i. EMS is hosted on platforms provided by third party cloud providers. We will have in place, maintain, and use information security measures, including physical, technical, and administrative controls, reasonably designed to prevent unauthorized access to EMS.

ii. We will maintain logical separation between the EMS cloud environment and Our internal business network.

iii. Our employees and subcontractors will use securely designed access methods to access EMS for support services.

iv. We will monitor EMS for indicators of unauthorized activity or compromise and have a dedicated security operations organization. We will retain logs of detection and blocking events for a minimum of one (1) year unless applicable law requires retention for a different period.

v. We will implement security measures engineered to facilitate a secure development lifecycle that is designed to systematically reduce the frequency and severity of vulnerabilities in code.

vi. We will utilize industry standard safeguards against Malware and malicious activity in EMS.

vii. We will not knowingly introduce Malware into EMS.

viii. We will implement and maintain security controls designed to protect EMS against known industry threats, such as the "OWASP Top 10" threats, via secure coding practices and appropriate technical controls.

5.2 Operating System/Applications.

i. We will implement and maintain change management procedures for EMS which include Our testing, certification, and approval processes specifically related to standard bug fixes, updates, security patches, and upgrades made available to You.

5.3 Backups.

i. We will perform and continuously maintain replication of a primary production site's Customer Data within the same country as the primary production site. Encryption of and access to Customer Data for the replicated sites must comply with this Annex.

ii. We will maintain a business continuity and/or disaster recovery plan in relation to the provision of EMS, which will be tested regularly.

iii. EMS leverages backups of its application and analytics data. The automated backup system is configured to perform daily incremental data backups of production databases.

5.4 Authentication/Authorization/Access.

i. We will require multi-factor authentication for all staff when gaining access to EMS, except where it is not technically possible.

ii. Supported authentication methods for Your Users are documented in Celonis product documentation.

iii. We will provide You with the option of multifactor authentication as documented in our product documentation.

iv. We will limit the number of Our support staff (including subcontractors) with persistent access to Customer Data consistent with the Principle of Least Privilege.

v. We will maintain an activity log of system access tracing such access back to specific employees of Ours who access the EMS production infrastructure, including those who may use administrator or other privileged access, on a central log server. We will implement and maintain a backup regime on the central log server. The retention period for such logs will be twelve (12) months. The activity log will be designed to include date and time, ID of who performed the action, resource accessed, event identifier, and event information. Log files will be immutable and inaccessible to administrators of the servers and resources being logged. We will regularly review logs related to the use of privileged access or anomalous security events (such as abnormal access attempts, critical data changes) to identify any irregularities.

5.5 Data Center Security.

i. EMS information-processing systems and supporting infrastructure will be located in data center facilities that meet Our requirements for physical security and provide an appropriate level of protection against unauthorized physical access, damage, and interference, which may include:

a. Physical access controls at building ingress points;

b. Identity controls of all visitors prior to sign-in;

c. Access control devices managing physical access to servers;

d. Regular review of physical access privileges;

e. Comprehensive monitor and alarm response procedures;

f. CCTV surveillance;

g. Appropriate fire detection and prevention systems;

h. Appropriate power redundancy and backup systems; and

i. Appropriate climate control systems.

5.6 Administrative Controls.

i. We will, to the extent legally permitted and in accordance with Our internal policies and processes, perform industry standard background checks on Our employees and subcontractors with access to Customer Data.

ii. Our employees are required to gain and maintain certification within Our security awareness and training program.

6. Data Deletion.

6.1 Within thirty (30) days of the expiry of Your Subscription Term or termination of the Agreement for any reason, and at Your request, We will either (i) securely destroy or render unreadable, undecipherable, or unrecoverable or (ii) deliver to You or Your designees all Customer Data or Confidential Information in Our possession, custody, or control.

7. Security Assessment and Testing

7.1 We will conduct, or commission third parties to conduct, at Our expense, vulnerability assessments and penetration testing of EMS regularly. Such assessments and testing will include validation of Our compliance with the security requirements herein and identification of security vulnerabilities, if any, of EMS. On request, We will share a confidential summary of scope and methodology of testing from the third party assessor.

7.2 You may, at Your own expense, conduct security assessments of Your EMS applications, but only in accordance with Our "Guidelines for Security Assessment by Customers". The following activities are expressly prohibited:

i. Denial of service (DoS). You are expressly prohibited from utilizing any tools or services in a manner that performs DoS attacks or simulations of such against any EMS asset;

ii. Resource request flooding (e.g. HTTP request flooding, Login request flooding, API request flooding);

iii. Protocol flooding (e.g. SYN flooding, ICMP flooding, UDP flooding);

iv. Scanning or testing assets belonging to any other customer;

v. Gaining access to any data that is not wholly-owned by You;

vi. Performing automated testing of services that generate significant amounts of traffic; and

vii. Attempting phishing or other social engineering attacks against Our employees.

7.3 We will take reasonable steps to mitigate and remediate any confirmed zero-day vulnerabilities detected or identified in EMS through patching, decommissioning or compensating controls.

8. Information Security Incident Detection and Response

8.1 Notice of Incident. In the event We become aware of any confirmed Information Security Incident materially and adversely affecting Your data, We will notify You without undue delay. Such notice will summarize in reasonable detail, to the extent known, a description of the nature of the breach, the likely consequences and the measures taken to address the breach. We will also advise details of a contact point where further information can be obtained.

8.2 Notice of Disclosure. We will provide You with copies of any public disclosure including filings, communications, general notices, press releases, or reports related to any Information Security Incident affecting Your data ("Communications"). Where the content of any such Communications identifies or may reasonably identify You, We will seek Your approval prior to the disclosure of such information, where permitted by law.

8.3 We will provide reasonable assistance with regards to any legally required reporting in response to any unauthorized access to EMS affecting Your data.

9. Customer Responsibilities

9.1 You are solely responsible for and shall take all reasonable steps to ensure appropriate administrative, technical, physical, organizational and operational safeguards are implemented and enforced for all areas under Your control, including but not limited to:

i. Ensuring that Customer Data for which HIPAA, FedRAMP or similar elevated security requirements apply is uploaded only to EMS instances specifically designated as appropriate for such data;

ii. Ensuring that payment card information is not uploaded or otherwise published to any EMS environment;

iii. Implementing all appropriate customer-configurable security controls to protect Your Customer Data;

iv. Implementing source system and Customer Data backups and appropriate data hygiene controls;

v. Ensuring any anonymization or pseudonymization tools (including those made available by Celonis) are configured properly;

vi. Safeguarding against Malware and other malicious activity, including without limitation scanning Your systems and Customer Data with current versions of industry-standard antivirus software and leveraging adequate firewall technologies;

vii. Monitoring and updating the Celonis status page to indicate incidents affecting availability (status.celonis.com). We will provide updates during the duration of any incident;

viii. Managing and protecting Your User roles and credentials; and

ix. Managing and protecting any encryption keys held by You to ensure the integrity, availability and confidentiality of the key and the Customer Data secured with such key.

9.2 You shall ensure that all Customer Data is subject to a regular backup cycle consistent with the nature of data being processed to ensure that data can be recovered in the event of any data loss, for which Celonis is not responsible. Recovery from backups shall be tested by You at least annually.