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.

Celonis Informationssicherheit Anhang

Dieser Anhang zur Informationssicherheit von Celonis (der "Anhang") legt die IT-Sicherheit und die Kontrollen fest, die für die Bereitstellung von EMS (wie unten definiert) durch Celonis gelten, und ist Bestandteil Ihrer Vereinbarung (einschließlich aller Bestellungen), die unsere Bereitstellung von EMS für Sie regelt (zusammenfassend die "Vereinbarung").

1. **Definitionen.** Alle in diesem Anhang in Großbuchstaben geschriebenen Begriffe haben die in der Vereinbarung festgelegte Bedeutung, sofern nachstehend nichts anderes bestimmt ist:
   1.1 **"EMS"** bezeichnet das Celonis Execution Management System, wie es Ihnen im Rahmen der Vereinbarung zur Verfügung gestellt wird.
   1.2 **"Hochverfügbarkeit"** bedeutet die Eliminierung einzelner Fehlerquellen, um den Betrieb von Anwendungen auch dann fortzusetzen, wenn eine der zugrunde liegenden IT-Komponenten ausfällt.
   1.3 **"Informationssicherheitsvorfall"** bedeutet jede(r) bestätigte (i) unbefugte Zugriff auf das EMS, dessen Veränderung oder Beschädigung oder (ii) Verlust oder unbefugte Veränderung oder Beschädigung von Kundendaten oder (iii) Diebstahl oder unbefugte Nutzung, Offenlegung oder Erwerb von oder Zugriff auf Kundendaten.
   1.4 **"Malware"** bezeichnet Programme oder Geräte (einschließlich Software, Codes oder Dateien), die den Zugang zu Computersoftware, Hardware oder Netzwerken, Telekommunikationsdiensten, -ausrüstungen oder -netzwerken oder anderen Diensten oder Geräten verhindern, beeinträchtigen oder den Betrieb, die Zuverlässigkeit oder die Benutzererfahrung anderweitig nachteilig beeinflussen sollen, einschließlich, aber nicht beschränkt auf Würmer, trojanische Pferde, Viren, Ransomware, Falltüren und andere ähnliche bösartige Programme .
   1.5 **"Grundsatz der geringsten Zugangsberechtigung "** bedeutet, dass Benutzern (oder Prozessen, die für Benutzer handeln) nur in dem Maße Zugang gewährt wird, wie es zur Erfüllung der ihnen zugewiesenen Aufgaben in Übereinstimmung mit den organisatorischen Aufgaben und Geschäftsfunktionen erforderlich ist.

2. **Unsere Verpflichtungen**
   2.1 Wir werden diesen Anhang einhalten und unsere Mitarbeiter ebenfalls dazu anhalten . Im Verhältnis zwischen Ihnen und Celonis sind wir für die Nichteinhaltung der in diesem Anhang festgelegten IT-Kontrollen durch unsere Unterauftragnehmer verantwortlich.
   2.2 Wir werden unsere umfassenden Regelungen zur Informationssicherheit in Übereinstimmung mit branchenweit anerkannten Standards und geltendem Recht aufrechterhalten. Diese Regelungen zur Informationssicherheit umfassen administrative, technische, physische, organisatorische und betriebliche Schutzmaßnahmen sowie andere Sicherheitsmaßnahmen, die (i) die Sicherheit und Vertraulichkeit von Kundendaten gewährleisten und (ii) die Bedrohung durch Informationssicherheitsvorfälle mindern sollen. Unsere Regelungen zur Informationssicherheit beinhalten auch ein Programm zur Sensibilisierung für Cybersicherheit, das die Mitarbeiter über vorbeugende Maßnahmen informiert und daran erinnert, um eine

3. Standards / Certifications .

3.1 We will maintain and will provide to You upon request and subject to confidentiality requirements, any then-available proof 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.

versehentliche Preisgabe von Kundendaten oder eine versehentliche Preisgabe von EMS für unbefugte Aktivitäten zu vermeiden.

2.3 Wir werden unsere Regelungen zur Informationssicherheit regelmäßig testen, überprüfen und aktualisieren.

3. Normen / Zertifizierungen .

3.1 Wir werden alle zu diesem Zeitpunkt verfügbaren Nachweise über die Einhaltung von Zertifizierungen und Standards aufbewahren und Ihnen auf Anfrage und vorbehaltlich der Vertraulichkeitsanforderungen zur Verfügung stellen, die unter anderem Folgendes umfassen können :

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 Sie können unsere aktuelle Liste der Zertifizierungen und des Konformitätsstatus unter http://trust.celonis.com/ einsehen.

4. Verschlüsselung.

4.1 Wir verschlüsseln Ihre Verbindung zu EMS mindestens mit einer Verschlüsselungl , die AES-128 (oder einem aktuellen gleichwertigen Branchenlevel) entspricht.

4.2 Wir verschlüsseln alle Kundendaten, die sich auf Backups befinden, mindestens mit einer Verschlüsselung , die AES-256 entspricht.

4.3 Wir verschlüsseln Kundendaten im Ruhezustand mit einer Verschlüsselung von mindestens AES-256 Bit. Die Daten werden verschlüsselt, unabhängig davon, ob der Hardware-Speicher ein- oder ausgeschaltet ist.

4.4 Wir werden Geheimnisse (d.h. Verschlüsselungsschlüssel, Zertifikate, Passwörter, Hashes) in einem geeigneten Dienst speichern. Wir speichern Systemgeheimnisse nicht in Konfigurationsdateien oder im Quellcode und setzen Zugangskontrollen ein, die gewährleisten , dass der Zugang zu solchen Informationen dem Prinzip der geringsten Zugangsberechtigung entspricht .

4.5 Wir verschlüsseln alle Passwörter mit einer Verschlüsselung , die mindestens AES-256 entspricht.

4.6 Wenn Sie eine private Cloud-Instanz erworben haben, unterstützen wir die Verwendung von Verschlüsselungsschlüsseln, die von Ihnen bereitgestellt werden (bringen Sie Ihren eigenen Verschlüsselungsschlüssel mit oder halten Sie ihn vor), und stellen Ihnen eine Möglichkeit zur Verfügung, den Schlüssel auszutauschen , wie in unserer jeweils aktuellen Produktdokumentation dokumentiert.

5. Kontrollen.

5.1 EMS.

i. Das EMS wird auf Plattformen gehostet, die von dritten Cloud-Anbietern bereitgestellt werden. Wir werden Maßnahmen zur Informationssicherheit, einschließlich physischer, technischer und administrativer Kontrollen, einrichten, aufrechterhalten und nutzen, die angemessen ausgestaltet sind, um einen unbefugten Zugriff auf EMS zu verhindern.

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.

ii. Wir werden eine logische Trennung zwischen der EMS-Cloud-Umgebung und unserem internen Geschäftsnetzwerk aufrechterhalten.

iii. Unsere Mitarbeiter und Subunternehmer werden sicher gestaltete Zugriffsmethoden verwenden, um für Supportdienstleistungen auf das EMS zuzugreifen.

iv. Wir werden EMS auf Anzeichen von unbefugten Aktivitäten oder Kompromittierung überwachen und verfügen über eine dedizierte Sicherheitsorganisation. Wir werden Protokolle von Erkennungs- und Blockierungsereignissen für mindestens ein (1) Jahr aufbewahren, es sei denn, das geltende Recht schreibt eine andere Aufbewahrungsfrist vor.

v. Wir setzen Sicherheitsmaßnahmen ein, die einen sicheren Entwicklungszyklus ermöglichen, der die Häufigkeit und den Schweregrad von Sicherheitslücken im Code systematisch reduziert.

vi. Wir werden branchenübliche Schutzmaßnahmen gegen Malware und bösartige Aktivitäten im EMS einsetzen.

vii. Wir werden nicht wissentlich Malware in das EMS einbringen .

viii. Wir werden Sicherheitskontrollen implementieren und aufrechterhalten, die darauf ausgelegt sind, EMS gegen bekannte Bedrohungen der Branche, wie z.B. die "OWASP Top 10" Bedrohungen, durch sichere Kodierungspraktiken und angemessene technische Kontrollen zu schützen.

5.2 Betriebssystem/Applikationen.

i. Wir werden Verfahren für Änderungsmanagement für EMS implementieren und aufrecht erhalten, die unsere Test-, Zertifizierungs- und Genehmigungsprozesse beinhalten, die sich speziell auf Standard-Fehlerbehebungen, Updates, Sicherheits -Patches und Upgrades beziehen, die Ihnen zur Verfügung gestellt werden.

5.3 Backups.

i. Wir werden Kundendaten eines primären Produktionsstandorts im selben Land wie der primäre Produktionsstandort replizieren und dies kontinuierlich aufrechterhalten. Die Verschlüsselung der Kundendaten und der Zugang zu ihnen für die replizierten Standorte müssen diesem Anhang entsprechen.

ii. Wir werden einen Geschäftskontinuitäts- und/oder Notfallwiederherstellungsplan in Bezug auf die Bereitstellung von EMS aufrechterhalten, der regelmäßig getestet wird.

iii. EMS nutzt Backups seiner Anwendungs- und Analysedaten. Das automatische Sicherungssystem ist so konfiguriert, dass es täglich inkrementelle Datensicherungen der Produktionsdatenbanken durchführt.

5.4 Authentifizierung/Berechtigung/Zugang.

i. Wir werden für alle Mitarbeiter eine Multi-Faktor-Authentifizierung für den Zugang zum EMS verlangen, es sei denn, dies ist technisch nicht möglich.

ii. Unterstützte Authentifizierungsmethoden für Ihre Benutzer sind in der Celonis Produktdokumentation dokumentiert.

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

iii. Wir werden Ihnen die Option der Multi-F aktor-Authentifizierung anbieten, wie in unserer Produktdokumentation dokumentiert.

iv. Wir begrenzen die Anzahl unserer Support-Mitarbeiter (einschließlich Subunternehmer) mit dauerhaftem Zugriff auf Kundendaten gemäß dem Grundsatz der geringsten Zugangsberechtigung .

v. Wir werden ein Aktivitätsprotokoll des Systemzugriffs auf einem zentralen Protokollserver führen, das den Zugriff auf bestimmte Mitarbeiter von uns zurückverfolgt, die auf die EMS-Produktionsinfrastruktur zugreifen, einschließlich derjenigen, die einen Administrator- oder anderen privilegierten Zugriff nutzen. Wir werden ein Sicherungssystem auf dem zentralen Protokollserver einführen und aufrechterhalten. Die Aufbewahrungsfrist für diese Protokolle beträgt zwölf (12) Monate . Das Aktivitätsprotokoll enthält Datum und Uhrzeit, die ID des Ausführenden, die Ressource, auf die zugegriffen wurde, die Ereigniskennung und die Ereignisinformation . Die Protokolldateien sind unveränderbar und für die Administratoren der protokollierten Server und Ressourcen unzugänglich. Wir überprüfen regelmäßig die Protokolle im Zusammenhang mit der Nutzung von privilegiertem Zugang oder anomalen Sicherheitsereignissen (wie anormale Zugriffsversuche, kritische Datenänderungen), um Unregelmäßigkeiten zu erkennen.

5.5 Sicherheit im Rechenzentrum.

i. Die EMS-Informationsverarbeitungssysteme und die unterstützende Infrastruktur werden in Rechenzentren untergebracht, die unsere Anforderungen an die physische Sicherheit erfüllen und ein angemessenes Maß an Schutz gegen unbefugten physischen Zugriff, Beschädigung und Störung bieten, was Folgendes beinhalten kann:

a. Physikalische Zugangskontrollen an den Gebäudeeingangspunkten;
b. Identitätskontrollen aller Besucher vor dem Einlass;
c. Zugangskontrollgeräte, die den physischen Zugang zu den Servern verwalten;
d. Regelmäßige Überprüfung der physischen Zugangsberechtigungen;
e. Umfassende Überwachungs- und Alarmreaktionsverfahren;
f. CCTV-Überwachung;
g. Geeignete Systeme zur Branderkennung und -verhütung;
h. Angemessene Stromredundanz und Backup-Systeme; und
i. Geeignete Klimakontrollsysteme.

5.6 Verwaltungskontrollen.

i. Wir führen, soweit gesetzlich zulässig und in Übereinstimmung mit unseren internen Richtlinien und Prozessen, branchenübliche Hintergrundüberprüfungen

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

bei unseren Mitarbeitern und Subunternehmern mit Zugang zu Kundendaten durch.

ii. Unsere Mitarbeiter sind verpflichtet, eine Zertifizierung im Rahmen unseres Sicherheitsbewusstseins- und Schulungsprogramms zu erlangen und aufrechtzuerhalten.

6. Löschung von Daten.

6.1 Innerhalb von dreißig (30) Tagen nach Ablauf Ihrer Abonnementlaufzeit oder der Beendigung der Vereinbarung aus irgendeinem Grund und auf Ihr Verlangen werden wir alle Kundendaten oder vertraulichen Informationen, die sich in unserem Besitz, Gewahrsam oder unter unserer Kontrolle befinden, entweder (i) sicher vernichten oder unleserlich, unentzifferbar oder nicht wieder herstellbar machen oder (ii) Ihnen oder Ihren Beauftragten aushändigen.

7. Bewertung und Prüfung der Sicherheit.

7.1 Wir werden auf unsere Kosten regelmäßig Schwachstellenanalysen und Penetrationstests des EMS durchführen oder durch Dritte durchführen lassen. Solche Bewertungen und Tests beinhalten die Überprüfung unserer Einhaltung der in diesem Anhang enthaltenen Sicherheitsanforderungen und die Identifizierung etwaiger Sicherheitsschwachstellen des EMS. Auf Anfrage werden wir Ihnen eine vertrauliche Zusammenfassung des Umfangs und der Methodik der Tests durch den Drittprüfer zur Verfügung stellen.

7.2 Sie können auf eigene Kosten Sicherheitsbewertungen Ihrer EMS-Anwendungen durchführen, jedoch nur in Übereinstimmung mit unseren "Richtlinien für Sicherheitsbewertungen durch Kunden". Die folgenden Aktivitäten sind ausdrücklich verboten:

i. Denial of Service (DoS). Es ist ausdrücklich untersagt, Werkzeuge oder Dienste zu benutzen, die DoS-Angriffe oder Simulationen solcher Angriffe gegen ein EMS-System durchführen;

ii. Ressourcen-Anfrage-Flooding (z.B. HTTP-Anfrage-Flooding, Login-Anfrage-Flooding, API-Anfrage-Flooding);

iii. Protokoll-Flooding (z.B. SYN-Flooding, ICMP-Flooding, UDP-Flooding);

iv. Scannen oder Testen von Anlagen, die einem anderen Kunden gehören;

v. Zugang zu Daten, die sich nicht vollständig in Ihrem Besitz befinden;

vi. Durchführung automatischer Tests von Diensten, die ein hohes Verkehrsaufkommen erzeugen; und

vii. Der Versuch von Phishing- oder anderen Social-Engineering-Angriffen gegen unsere Mitarbeiter.

7.3 Wir werden angemessene Schritte unternehmen, um alle bestätigten Zero-Day-Schwachstellen, die im EMS entdeckt oder identifiziert wurden, durch Patches, Stilllegung oder kompensierende Kontrollen zu entschärfen und zu beheben.

8. Erkennung von und Reaktion auf Informationssicherheitsvorfälle

8.1 Benachrichtigung über einen Vorfall. Sollten wir Kenntnis von einem bestätigten Informationssicherheitsvorfall erlangen, der sich wesentlich und nachteilig auf Ihre Daten auswirkt, werden wir Sie unverzüglich benachrichtigen. Eine solche Benachrichtigung wird,

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.

soweit bekannt, in angemessener Ausführlichkeit eine Beschreibung der Art des Verstoßes, der wahrscheinlichen Folgen und der zur Behebung des Verstoßes getroffenen Maßnahmen enthalten. Wir werden Ihnen auch eine Kontaktstelle nennen, bei der Sie weitere Informationen erhalten können.

8.2 Bekanntgabe der Offenlegung. Wir stellen Ihnen Kopien aller öffentlichen Bekanntmachungen zur Verfügung, einschließlich Einreichungen, Mitteilungen, allgemeiner Bekanntmachungen, Pressemitteilungen oder Berichte im Zusammenhang mit einem Informationssicherheitsvorfall, der Ihre Daten betrifft ("Mitteilungen"). Wenn der Inhalt solcher Mitteilungen Sie identifiziert oder angemessenerweise identifizieren könnte, werden wir vor der Offenlegung solcher Informationen Ihre Zustimmung einholen, sofern dies gesetzlich zulässig ist.

8.3 Wir unterstützen Sie in angemessener Weise bei der gesetzlich vorgeschriebenen Berichterstattung über einen unbefugten Zugriff auf EMS, der Ihre Daten betrifft.

9. Verantwortlichkeiten des Kunden

9.1 Sie sind allein dafür verantwortlich und müssen alle angemessenen Schritte unternehmen, um sicherzustellen, dass angemessene administrative, technische, physische, organisatorische und betriebliche Sicherheitsmaßnahmen für alle Bereiche unter Ihrer Kontrolle implementiert und durchgesetzt werden, einschließlich aber nicht beschränkt auf:

i. Sicherstellung, dass Kundendaten, für die HIPAA-, FedRAMP- oder ähnliche erhöhte Sicherheitsanforderungen gelten, nur auf EMS-Instanzen hochgeladen werden, die speziell für solche Daten als geeignet ausgewiesen sind;

ii. Sicherstellung, dass Zahlungskarteninformationen nicht in eine EMS-Umgebung hochgeladen oder anderweitig veröffentlicht werden;

iii. Die Implementierung aller angemessenen, vom Kunden konfigurierbaren Sicherheitskontrollen zum Schutz Ihrer Kundendaten;

iv. Implementierung von Sicherungskopien des Quellsystems und der Kundendaten und angemessene Kontrollen der Datenhygiene;

v. Sicherstellung, dass alle Anonymisierungs- oder Pseudonymisierungstools (einschließlich der von Celonis zur Verfügung gestellten) richtig konfiguriert sind;

vi. Schutz vor Malware und anderen bösartigen Aktivitäten, einschließlich, aber nicht beschränkt auf das Scannen Ihrer Systeme und Kundendaten mit aktuellen Versionen von branchenüblicher Antivirensoftware und dem Einsatz angemessener Firewall-Technologien;

vii. Überwachung und Aktualisierung der Celonis-Statusseite, um Vorfälle anzuzeigen, die die Verfügbarkeit beeinträchtigen (status.celonis.com). Wir werden während der Dauer eines Vorfalls Updates zur Verfügung stellen;

viii. Verwaltung und Schutz Ihrer Benutzerrollen und Anmeldedaten; und

ix. Verwaltung und Schutz aller von Ihnen gehaltenen Verschlüsselungsschlüssel, um die Integrität, Verfügbarkeit

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.

und Vertraulichkeit des Schlüssels und der mit diesem Schlüssel gesicherten Kundendaten sicherzustellen.

9.2 Sie stellen sicher, dass alle Kundendaten einem regelmäßigen Sicherungszyklus unterliegen, der der Art der verarbeiteten Daten entspricht, um sicherzustellen, dass die Daten im Falle eines Datenverlustes, für den Celonis nicht verantwortlich ist, wiederhergestellt werden können. Die Wiederherstellung aus Sicherungskopien ist von Ihnen mindestens einmal jährlich zu testen.

This German version is a translation of the original in English, and is provided for informational purposes only. In case of any ambiguity or discrepancy, the English original will prevail.

Diese deutsche Version ist eine Übersetzung des englischen Originals und dient lediglich zu Informationszwecken. Im Falle von Unklarheiten oder Abweichungen ist das englische Original maßgebend.