KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Technische und Organisatorische Sicherheitsmaßnahmen bei Krones(Technical and Organizational Security Measures at Krones “TOMs“)

Teil A - Allgemeine technische und organisatorische Sicherheitsmaßnahmen bei Krones (General technical and organizational security measures at KRONES „GTOMs)

Beschreibung der technischen und organisatorischen Maßnahmen, die in Übereinstimmung mit Artikel 32 der DSGVO übernommen werden

Die Krones AG hat zum Schutz personenbezogener Daten ein umfangreiches Paket an technischen und organisatorischen Maßnahmen implementiert und verbessert diese kontinuierlich. Dieser Teil gibt eine Übersicht über allgemeine Maßnahmen, die für grundlegende Verarbeitungen in allen unseren digitalen Diensten gelten. Für bestimmte digitale Produkte oder Dienste können spezifische technische und organisatorische Sicherheitsmaßnahmen (servic specific technical and organizational security measures „STOMs“) diese allgemeinen Maßnahmen ergänzen.

Krones hat ein konzernübergreifendes Informationssicherheits-Managementsystem (ISMS) und Datenschutz-Managementsystem (DPMS) eingerichtet. ISO/IEC 27001 dient hierbei als Leitlinie für das ISMS. Krones hat einen Corporate Information Security Officer und einen Datenschutzbeauftragten ernannt. Durch regelmäßige Datenschutz- und Informationssicherheitsschulungen werden die Mitarbeiter bezüglich Datenschutz und Informationssicherheit geschult. Alle Mitarbeiter, die in Kontakt mit personenbezogenen Daten kommen, verpflichten sich zu Vertraulichkeit und Geheimhaltung der Daten, in Übereinstimmung mit Art. 28 Abs. 3 Satz 2 Buchstabe b, 29, 32 Abs. 4 DSGVO.

Die internen IT-Services des Informationsmanagements der Krones AG sind die Grundlage für unsere Entwicklungs-, Wartungs- und Betriebsaktivitäten. Das Krones Informationsmanagement ist nach ISO/IEC 27001 zertifiziert. Die Richtlinien und Leitlinien von Krones orientieren sich an internationalen Standards und Best-Practice-Ansätzen, um ein angemessenes Informationssicherheitsniveau sicherzustellen. Das Unternehmen hält sich an die Vorschriften zum Schutz personenbezogener Daten, insbesondere an die in der DSGVO angegebenen, soweit diese anwendbar sind.

Die folgenden technischen und organisatorischen Maßnahmen wurden ergriffen, um die Anforderungen nach Artikel 32 DSGVO zu erfüllen.

I. Grundsätze Pseudonymisierung, Verschlüsselung, Informationssicherheit und Datenschutz durch Technikgestaltung

Nach den Grundsätzen der Pseudonymisierung und Anonymisierung und soweit personenbezogene Daten nicht für den Zweck einer Verarbeitungstätigkeit erforderlich sind, werden Daten in nicht personenbezogener Form verarbeitet und genutzt. Der Einsatz von hochmodernen Verschlüsselungstechnologien erfolgt auf der Grundlage der internen Informationsverwendungsrichtlinie und der Leitlinien für den Einsatz von kryptographischen Algorithmen. Die frühzeitige Einbeziehung von Informationssicherheits- und Datenschutzanforderungen bei der Gestaltung und Änderung von Diensten („Security & Privacy by Design") stellt Maßnahmen und ein dem Risiko angemessenes Sicherheitsniveau sicher.

II. Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten

Die Krones AG hat folgende Maßnahmen ergriffen, um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

1) Maßnahmen zur Vertraulichkeit
Zutrittskontrolle

Der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet und genutzt werden, ist Unbefugten verwehrt.
Maßnahmen:

- Zutritt zu Geschäftsräumen und Rechenzentren nur für autorisierte Personen Geschäftsräume werden vom Werkschutz bewacht
- Elektronische Zutrittskontrolle mittels Firmenausweis mit Transponder-Chip
- Verwaltung aller Zugriffsrechte mit einem Zugriffskontrollsystem
- Zugang zu Rechenzentren nur mit einer Zwei-Faktor-Authentifizierung
- Einbruchmeldeanlage für die Rechenzentren
- Zugangsberechtigungsverfahren für Externe (Dokumentation der Erlaubnis und Vorlage des Personalausweises)

IT-System-Zugangskontrolle
Verhinderung des Zugangs auf Datenverarbeitungssysteme durch Unbefugte.
Maßnahmen:

- Zugang zu Servern und Clients mit Authentifizierung über eine individuelle Benutzer-ID und ein Passwort (erzwungene Passwortsicherheit)
- Passwortsicherheitsleitlinie gemäß Best Practice mit Komplexitätsanforderungen und regelmäßigen Passwortänderungen
- Schutz des internen Netzwerks vor unbefugtem Zugriff durch Firewall und Antiviren-Software
- Zugriff auf Clients über Remote Service nur für autorisierte Personen und mit Genehmigung des Nutzers
- Fernzugriff auf das interne Netzwerk nur über VPN/Citrix unter Verwendung einer Zwei-Faktor-Authentifizierung
- Einsatz eines Mobile Device Management Systems

Datenzugriffskontrolle
Personen, die zur Nutzung eines automatisierten Verarbeitungssystems berechtigt sind, haben nur Zugang zu den personenbezogenen Daten, für die sie eine Zugriffsberechtigung besitzen.
Maßnahmen:

- Rechte- und rollenbasiertes Zugriffskontrollsystem
- Zuweisung von Berechtigungen nach dem Need-to-know-Prinzip
- Zentralisiertes Berechtigungsmanagement und Identitäts- und Zugriffsmanagement mit entsprechenden Prozessen
- Getrennte persönliche Konten für Verwaltungszwecke
- Protokollierung des Zugriffs
- Konzept zur Sicherung und Wiederherstellung
- Regelmäßige interne und externe Audits zur Überprüfung der Maßnahmen zur Zugriffskontrolle

Trennbarkeit
Personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, können getrennt verarbeitet werden.
Maßnahmen:

- Logisch getrennte Speicherung von Daten verschiedener Auftraggeber in unseren digitalen Services
- Regelung von Zugriffsberechtigungen auf Basis von Gruppenrichtlinien und Verzeichnisstrukturen

2) Maßnahmen zur Integrität
Übertragungskontrolle
Personenbezogene Daten können bei der elektronischen Übertragung oder beim Transport von Datenträgern nicht gelesen, kopiert, verändert oder entfernt werden.
Maßnahmen:

- Entsorgung von Datenträgern und Informationen durch ein dafür zertifiziertes Unternehmen
- Verschlüsselte Mediengeräte unter Verwendung modernster Verfahren

- Klassifizierungsebenen für Informationen und angemessene Behandlung gemäß den Leitlinien
- Verschlüsselte VPN Verbindungen
- Übertragung von Daten über verschlüsselte Verbindungen (z. B. TLS)
- Optionale Lösung für E-Mail-Verschlüsselung

Eingabekontrolle

Es kann anschließend überprüft und festgestellt werden, welche personenbezogenen Daten in automatisierte Verarbeitungssysteme eingegeben wurden und wann und von wem die personenbezogenen Daten eingegeben wurden.
Maßnahmen:

- Protokollierung sensibler Aktionen und Ereignisse in kritischen Systemen
- Authentifizierung über individuelle Benutzer-ID
- Differenzierte Zuweisung von Berechtigungen

3) Maßnahmen zu Verfügbarkeit, Ausfallsicherheit und Wiederherstellung

Sicherstellung der Verfügbarkeit

Personenbezogene Daten werden vor Verlust und Zerstörung geschützt.
Maßnahmen:

- Physische Sicherheit der Rechenzentren (z. B. USV, Brandschutz, Einbruchmeldeanlage, Kühlanlage)
- Redundante Rechenzentren
- Redundante Stromversorgung und Netzwerkanbindung der Rechenzentren
- Hard- und Softwareschutz (z. B. Virenscanner, Firewall, redundante USV, Kühlanlage)
- Sichere Löschung und Entsorgung von Datenträgern und IT-Geräten auf der Grundlage einer internen Arbeitsanweisung zur sicheren Löschung und Vernichtung (in Anlehnung an DIN-66399)

Wiederherstellung der Verfügbarkeit

Die installierten Systeme können bei einer Unterbrechung wiederhergestellt werden.
Maßnahmen:

- IT Service Continuity Management Prozesse und regelmäßige Notfallübungen
- Notfall- und Wiederherstellungspläne für zentrale IT-Dienste
- Sicherungs- und Wiederherstellungskonzept mit täglicher Datensicherung

III. Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung von technischen und organisatorischen Maßnahmen

Informationssicherheits- und Datenschutzmanagementsystem

Die implementierten technischen und organisatorischen Sicherheitsmaßnahmen werden im Rahmen des ISMS und DPMS regelmäßig getestet, bewertet und evaluiert, um eine kontinuierliche Verbesserung zu gewährleisten.
Maßnahmen:

- ISMS auf der Grundlage von ISO 27001 und IT-Servicemanagement auf der Grundlage von ISO 20000
- Informationssicherheitsrichtlinie als übergeordnetes Dokument mit detaillierten Unterrichtlinien für alle relevanten Bereiche
- Interne und externe Audits zur regelmäßigen Prüfung, Beurteilung und Bewertung der umgesetzten technischen und organisatorischen Maßnahmen
- Regelmäßige technische Überprüfung und Instandhaltung der zentralen IT-Systeme
- Schwachstellen- und Penetrationstests für IT-Systeme durch unser internes Sicherheitsteam und mit externen Partnern
- Information Security Incident Response Process Team (ISIRT) zur Bearbeitung und Koordinierung von Sicherheitsvorfällen

- Product Security Incident Response Team (PSIRT) zur Bearbeitung und Koordinierung von produktbezogenen Sicherheitsereignissen und -vorfällen und zur Bereitstellung von Sicherheitsempfehlungen für Kunden
- Kontinuierlicher Verbesserungsprozess für unser Managementsystem

Verarbeitungskontrolle

Personenbezogene Daten, die im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet werden, können nur gemäß den Anweisungen des für die Verarbeitung Verantwortlichen verarbeitet werden.

Maßnahmen:

- Lieferantenmanagementprozess und Prozess zur Bewertung und Auswahl von Lieferanten, insbesondere Leitlinien für die Nutzung von Cloud Services und Checklisten für Anbieter von Cloud Services
- Ansprechpartner und Auftragsbestätigungen sind schriftlich bereitzustellen und müssen die Pflichten, Aufgaben und Arbeitsanweisungen des Kunden und des Lieferanten enthalten
- Die mit der Verarbeitung beschäftigten Mitarbeiter werden über die Kundenspezifikation und die spezifischen Arbeitsanweisungen informiert
- Mitarbeiter, die mit der Verarbeitung beschäftigt sind, werden zur Vertraulichkeit verpflichtet und regelmäßig zu Datenschutz und Informationssicherheit geschult
- Datenschutzvereinbarungen mit Unterauftragsverarbeitern, die mit der Verarbeitung personenbezogener Daten gemäß Art. 28 DSGVO und/oder durch Vereinbarung auf der Grundlage geeigneter Garantien für die Verarbeitung durch Unterauftragsverarbeiter in einem Drittland (siehe Art. 28 Abs. 4) betraut wurden

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Teil B - Servicespezifische technische und organisatorische Sicherheitsmaßnahmen (Service specific technical and organizational security measures “ STOMs”)

STOMs für LCS Support

Die Krones AG setzt bei der Bereitstellung der IT-Services Argos (Augmented Reality Support) und GRS (Global Remote Service) auf ein mehrstufiges Konzept. Der Großteil des IT-Dienstes GRS (Global Remote Service) wird auf Servern erbracht, die im Rechenzentrum der Krones AG betrieben werden. Einzelne Teile der IT-Dienste Argos (Augmented Reality Support) und GRS (Global Remote Service) werden als „Managed Services“ von Drittanbietern bezogen. Der Remote Service wird von speziell für den Remote Service geschulten Mitarbeitern der Krones AG erbracht. Zum Erreichen eines hohen Maßes an Datensicherheit wählt die Krones AG ihre Lieferanten sorgfältig aus, schließt mit ihnen Datenverarbeitungsverträge ab und überwacht deren Einhaltung im Rahmen ihrer ISMS-Aktivitäten.

STOMs für Digital Services

Die Share2Act Digital Services werden von der Syskron GmbH im Auftrag der Krones AG entwickelt und betrieben. Die Share2Act Digital Services basieren auf der Plattform und den Services von Amazon Web Services. Syskron hat zum Schutz personenbezogener Daten innerhalb der Share2Act Digital Services umfangreiche technische und organisatorische Maßnahmen umgesetzt.

I. Grundsätze Pseudonymisierung, Verschlüsselung, Informationssicherheit und Datenschutz durch Technikgestaltung

Nach den Grundsätzen der Pseudonymisierung und Anonymisierung und soweit personenbezogene Daten nicht für den Zweck einer Verarbeitungstätigkeit erforderlich sind, werden Daten in nicht personenbezogener Form verarbeitet und genutzt. Der Einsatz von hochmodernen Verschlüsselungstechnologien und der Best Practices erfolgt auf der Grundlage der internen Informationsverwendungsrichtlinie und der Leitlinien für den Einsatz von kryptographischen Algorithmen. Die frühzeitige Einbeziehung von Informationssicherheits- und Datenschutzanforderungen bei der Gestaltung und Änderung von Diensten („Security & Privacy by Design") stellt Maßnahmen und ein dem Risiko angemessenes Sicherheitsniveau sicher.

II. Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten

Die folgenden Maßnahmen wurden ergriffen, um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen.

Datenzugriffskontrolle

Personen, die zur Nutzung eines automatisierten Verarbeitungssystems berechtigt sind, haben nur Zugang zu den personenbezogenen Daten, für die sie eine Zugriffsberechtigung besitzen.

Maßnahmen:

- Zuweisung von Berechtigungen nach dem Need-to-know-Prinzip
- Getrennte persönliche Konten für Verwaltungszwecke
- Konzept zur Sicherung und Wiederherstellung

Trennbarkeit

Personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, können getrennt verarbeitet werden.

Maßnahmen:

- Logisch getrennte Speicherung von Daten verschiedener KUNDEN.
- Konzept und Struktur von Zugangskontrolle und Zugang von Mietern.

Eingabekontrolle

Es kann anschließend überprüft und festgestellt werden, welche personenbezogenen Daten in automatisierte Verarbeitungssysteme eingegeben wurden und wann und von wem die personenbezogenen Daten eingegeben wurden.

Maßnahmen:

- Protokollierung und bedarfsgerechte Bereitstellung entsprechender Aktionen auf Systemen (z. B. Logfiles)
- Authentifizierung über individuelle Benutzer-ID
- Differenzierte Zuweisung von Berechtigungen

Absicherung der Verfügbarkeit

Personenbezogene Daten werden vor Verlust und Zerstörung geschützt.

Maßnahmen:

- Redundantes Rechenzentrum unserer Hosting-Partner
- Redundante Datenspeicherung bei unseren Hosting-Partnern
- Löschung von Daten nach den gesetzlichen Bestimmungen und Kundenanforderungen

Ausfallsicherheit von Systemen

Wir ergreifen präventive Maßnahmen, die bereits vor der Durchführung der Datenverarbeitung durch die Auftragsverarbeiter zur Stabilität der Systeme beitragen.

Maßnahmen:

- Nutzung des Lastausgleichs des Netzwerkverkehrs auf dem Server
- Durchführung von wiederkehrenden Penetrationstests gegen die Datenverarbeitungssysteme
- Automatische Anpassung von Rechenleistung, Speicher und Arbeitsspeicher

Wiederherstellung der Verfügbarkeit

Wir gewährleisten die Verfügbarkeit durch Wiederherstellbarkeit durch implementierte Disaster-Recovery-Pläne.

Maßnahmen:

- Regelmäßige Archivierung und separate Speicherung von Datenbeständen in Kombination mit einer Server-Spiegelung unseres Hosting-Partners
- Backup-Konzept mit täglicher Datensicherung

III. Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung von technischen und organisatorischen Maßnahmen

Wir führen Maßnahmen durch, um die bestehenden technischen und organisatorischen Maßnahmen zu überprüfen und auf dem neuesten Stand zu halten.