Technische und organisatorische Maßnahmen zum Datenschutz

in Anlehnung an den Wortlaut des Gesetzes 110/2019 Slg. über die Verarbeitung personenbezogener Daten,
und Artikel 32 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (GDPR)

Inhalt:

Revisionsunterlagen dokumentieren:

Datum der Überarbeitung:	Ergebnis:	Er hat die Prüfung durchgeführt:
18.6.2018	Datenzugriffskontrolle aktualisieren - Kontosperrung	Z. Sedlak
25.6.2019	Gesamtüberprüfung nach dem Inkrafttreten des Gesetzes 110/2019 Slg. über die Verarbeitung personenbezogener Daten	Z. Sedlak
25.11.2019	Beschreibung der VLAN-Trennung hinzugefügt	Z. Sedlak
23.8.2021	Geänderte Beschreibung der Kennwortrichtlinie - Änderung aufgrund der Migration von Client-PCs in eine neue Domäne	Z. Sedlak
23.8.2021	Zusätzliche MFA-Sicherheit für die Benutzerauthentifizierung in Microsoft-Cloud-Diensten (Outlook, Teams)	Z. Sedlak
7.6.2024	Geänderte Beschreibung der Passwort-Richtlinie und des Intervalls für die Bildschirmsperre entsprechend der neuen Domain-Richtlinie, Korrektur der deutschen Übersetzung	Z. Sedlak

PARAGON

1 Umfang der Gültigkeit

Sie gilt für alle Mitarbeiter und Personen, die für oder im Namen der Organisation arbeiten und von der Organisation verwaltet werden (im Folgenden als Mitarbeiter oder Person bezeichnet).

2 Gesetzgeberischer Rahmen

2.1 Gesetz 110/2019 Slg. über die Verarbeitung von personenbezogenen Daten

§ 40 - Sicherheit der Verarbeitung personenbezogener Daten

(1) Die Verwaltungsbehörde trifft die organisatorischen und technischen Maßnahmen, die erforderlich sind, um ein der Art, dem Umfang, den Umständen, dem Zweck und dem Risiko der Verarbeitung angemessenes Maß an Sicherheit der personenbezogenen Daten zu gewährleisten.

(2) Werden personenbezogene Daten im automatisierten Verfahren verarbeitet, so trifft die Verwaltungsbehörde die erforderlichen Maßnahmen, um

(a) diese personenbezogenen Daten vor unbefugtem Zugriff, unbefugter Weitergabe, Veränderung, Vernichtung, Verlust, Diebstahl, Missbrauch oder sonstiger unbefugter Verarbeitung zu schützen,

(b) die Wiederauffindbarkeit dieser personenbezogenen Daten zu gewährleisten,

(c) zu gewährleisten, dass die Person, die die personenbezogenen Daten eingegeben hat oder der die personenbezogenen Daten über das Datenübertragungsgerät übermittelt oder zur Verfügung gestellt wurden, identifiziert und überprüft werden kann,

(d) die Sicherheit und Zuverlässigkeit des Informationssystems, das die personenbezogenen Daten enthält, zu gewährleisten, einschließlich der Meldung von Fehlern, und

(e) den unbefugten Zugang zu den Speichermedien oder Geräten zu verhindern, die für die Verarbeitung dieser personenbezogenen Daten verwendet werden.

(3) Die Verpflichtungen der Verwaltungsbehörde nach den Absätzen 1 und 2 gelten entsprechend für den Auftragsverarbeiter.

§ 46 - Pflichten der Personen bei der Sicherung personenbezogener Daten

(1) Der für die Verarbeitung Verantwortliche hat technische und organisatorische Maßnahmen zu treffen, um zu verhindern, dass personenbezogene Daten unbefugt oder zufällig abgerufen, verändert, zerstört, verloren oder in sonstiger Weise unbefugt übermittelt oder missbraucht werden. Diese Verpflichtung gilt auch nach Beendigung der Verarbeitung personenbezogener Daten.

(2) Der für die Verarbeitung Verantwortliche ist verpflichtet, technische und organisatorische Maßnahmen zu treffen, um den Schutz personenbezogener Daten nach Maßgabe des Gesetzes und anderer Rechtsvorschriften zu gewährleisten. Der für die Verarbeitung Verantwortliche führt eine Dokumentation über die getroffenen technischen und organisatorischen Maßnahmen und bewahrt sie während der Dauer der Verarbeitung personenbezogener Daten auf.

(3) Im Rahmen der in Absatz (1) genannten Maßnahmen bewertet der Verwalter die Risiken in Bezug auf Bereiche

(a) die Einhaltung von Anweisungen für die Verarbeitung personenbezogener Daten durch Personen, die direkten Zugang zu personenbezogenen Daten haben,

(b) Verhinderung des Zugriffs Unbefugter auf personenbezogene Daten und auf die Mittel zu ihrer Verarbeitung,

(c) die Verhinderung des unbefugten Lesens, Erstellens, Kopierens, Übertragens, Änderns oder Löschens von Aufzeichnungen mit personenbezogenen Daten; und

(d) Maßnahmen zur Feststellung und Überprüfung, an wen die personenbezogenen Daten übermittelt wurden.

(4) Im Falle einer automatisierten Verarbeitung personenbezogener Daten ist der für die Verarbeitung Verantwortliche im Rahmen der in Absatz 1 genannten Maßnahmen auch dazu verpflichtet

(a) Sie stellen sicher, dass nur befugte natürliche Personen das System zur automatisierten Verarbeitung personenbezogener Daten nutzen,

(b) sicherzustellen, dass die befugte natürliche Person nur Zugang zu den ihrer Befugnis entsprechenden personenbezogenen Daten hat, und zwar auf der Grundlage einer ausschließlich für diese Person erteilten besonderen Nutzungsberechtigung,

(c) elektronische Aufzeichnungen anzufertigen, die es ermöglichen, festzustellen und zu überprüfen, wann, von wem und aus welchem Grund personenbezogene Daten aufgezeichnet oder anderweitig verarbeitet worden sind, und

(d) den unbefugten Zugang zu Datenträgern zu verhindern.

(5) Die Verpflichtungen nach den Absätzen 1 bis 4 gelten entsprechend für Verarbeiter.

2.2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (GDPR)

Abschnitt 2 - Sicherheit der personenbezogenen Daten, Artikel 32 - Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

(a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten; 4.5.2016 DE Amtsblatt der Europäischen Union L 119/51

(b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

(c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

(d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

3 Durchgeführte technische und organisatorische Maßnahmen

Paragon Customer Communications Czech Republic a.s. hat die folgenden technischen und organisatorischen Maßnahmen im Rahmen der geltenden Gesetzgebung, auf die in Punkt 2 dieses dokumentierten Verfahrens Bezug genommen wird, eingerichtet, umgesetzt und überwacht regelmäßig deren Einhaltung.

Die regelmäßige Kontrolle und Überprüfung der technischen und organisatorischen Maßnahmen erfolgt im Rahmen des Informationssicherheitsmanagementsystems nach ISO 27001:2022. DI **ISMS-DP01-Planung, Betrieb und Management von ISMS**.

3.1 Physische Zugangskontrolle

Die Büros der Organisation befinden sich am Hauptsitz des Unternehmens, in
Dr. Pavla Klementa 1082, 330 23, Nýřany

- Der physische Zugang zu den Einrichtungen ist eingeschränkt und wird durch ein Schlüsselsystem kontrolliert.
- Der Zugang zu den Datenverarbeitungsanlagen wird durch eine besondere Zugangsberechtigung (Extra-Schlüssel, oder.

  elektronisches Zugangssystem)
- Jede Ankunft einer externen Einheit auf dem Gelände der Organisation wird angekündigt und protokolliert
- Die Räumlichkeiten sind logisch getrennt, der Zugang einer externen Einheit ist so weit wie möglich eingeschränkt.
- Es gibt ein obligatorisches Verriegelungssystem
- Der physische Zugang zu den Servern und aktiven Elementen von ist nur autorisierten Mitarbeitern (oder Personen, die einen entsprechenden Vertrag für die Verwaltung dieser Einrichtungen abgeschlossen haben) gestattet.
- In separaten (eigenen) Räumen können diese technischen Geräte frei platziert werden.
- Befinden sich die technischen Einrichtungen in Räumen, die auch für andere Zwecke als den Standort der technischen Einrichtungen genutzt werden, müssen die Einrichtungen in einem abschließbaren Schrank untergebracht werden. Nur Personen, die für die technischen Anlagen zuständig sind, dürfen die Schlüssel haben.
- Es gibt ein Kamerasystem zur Überwachung der Bewegungen von Personen und Materialien außerhalb des Gebäudes
- Sicherheit ist 24/7 verfügbar

3.2 Datenzugangskontrolle (Authentifizierung)

- ISMS-Grundsätze für Vertraulichkeit, Verfügbarkeit und Integrität von Daten sind vorhanden, die Grundsätze des geringsten "least-privilege" und „need-to-know“.Der Zugriff auf die Daten wird über Benutzerkonten gesteuert
- Jeder Benutzer verwendet eine eindeutige Kennung (ID, Name)

- Die Authentifizierung dient dazu, die Identität eines Benutzers zu überprüfen und den Benutzer zu autorisieren, die gewünschten Dienste in Anspruch zu nehmen und auf Anwendungen und Daten zuzugreifen.
- Passwortpolitik ist definiert (Passwortlänge mindestens 12 Zeichen, Passwort muss (soweit technisch möglich) die Komplexitätsanforderungen erfüllen (3 von 4 Kriterien), Benutzer müssen ihr Passwort nach dem ersten Login ändern, Passwortgültigkeit beträgt 120 Tage, die letzten 13 Passwörter müssen unterschiedlich sein
- Multi-Faktor-Authentifizierung (MFA) ist implementiert, um den Zugriff auf Microsoft Cloud-Dienste (Exchange, MS Team) zu authentifizieren.
- Die automatische Bildschirmsperre ist auf 5 Minuten eingestellt.
- Die Einrichtung und Löschung von Benutzerkonten sowie die Festlegung von Berechtigungen werden von den jeweiligen Vorgesetzten genehmigt.
- Der externe Zugriff auf die Daten wird über verschlüsselte SFTP-Dienste, VPN SSL, durch die Unternehmensfirewall (Zugriff über IP-Adresse) und eine eindeutige Benutzeridentifizierung (Name + Passwort oder Zertifikat) kontrolliert.
- Die IT-Infrastruktur ist durch Firewall und definierte VPNs vor unberechtigtem Zugriff geschützt
- Die IT-Infrastruktur ist durch Antivirenprogramme vor Sicherheitsbedrohungen geschützt, und es werden Maßnahmen zur Bekämpfung von Ransomware auf der Ebene der Firewall und der Domänenrichtlinien getroffen.

3.3 Hardware-Zugangskontrolle (Autorisierung)

- Der Benutzer hat nur Zugriff auf die definierten Computer (Active Directory-Einstellungen)
- Eine eindeutige Kennung (Active Directory-Konto) wird für den Zugriff auf den PC verwendet
- Der Lese-/Schreibzugriff auf den HW-Computer (USB-Laufwerk, Flash-Laufwerk, Digifoto) wird durch Domänenrichtlinien gesteuert.
- Der Zugriff auf Netzlaufwerke basiert auf Benutzerberechtigungen (Active Directory) oder Passwörtern (iSCSI Target)
- Anonyme Konten sind nicht erlaubt
- Externe Anbieter haben maximal eingeschränkten Zugang (Active Directory-Konto)

3.4 Datenübertragung (Verschlüsselung)

- Die Daten dürfen nur über einen sicheren Weg übertragen werden, wobei die Verschlüsselungsmethode auch von der Gegenpartei abhängig ist.
- Die Verschlüsselungsmethode ist Teil des geschlossenen Verarbeitungsvertrags
- Personenbezogene Daten dürfen nicht per E-Mail-Kommunikation übermittelt werden
- Beim Datenaustausch über digitale Medien (DVD, USB) ist das Mindestmaß an Verschlüsselung ein verschlüsseltes Archiv, das Passwort muss den Kriterien eines starken Passworts entsprechen, das Passwort wird dem Empfänger über einen anderen Kommunikationskanal, z. B. E-Mail oder SMS, mitgeteilt.

- Bei der automatischen Datenübertragung wird die verschlüsselte Datenübertragung per SFTP oder VPN verwendet. Die SFTP-Verschlüsselung basiert auf RSA 4096 Bit, VPN verwendet SSL (SHA2 4096 Bit).

3.5 Systemprotokollierung und -überwachung

- Die Protokollierung aller Systeme wird kontinuierlich durchgeführt. Die Mitarbeiter sind verpflichtet, den Sicherheitsbeauftragten zu informieren, wenn eine Störung oder ein Zwischenfall festgestellt wird.
- Die Überwachung der Nutzeraktivitäten wird fortgesetzt. Es werden Aufzeichnungen geführt, die, soweit möglich, Folgendes enthalten:
    - Benutzer Identifikatoren (Benutzer-IDs)
    - Datum und Uhrzeit der An- und Abmeldung
    - eine Aufzeichnung der erfolgreichen und abgelehnten Zugriffsversuche auf das System
    - Verwendung von privilegierten Konten
    - eine Aufzeichnung der abgelehnten Versuche, auf Daten und andere Ressourcen zuzugreifen.
    - Änderungen der Systemkonfiguration
- Die Überwachung und Protokollierung des Datenverkehrs durch die Unternehmensfirewall wird fortgesetzt.

3.6 Kontrolle der Verarbeitung

- Aufträge werden auf der Grundlage einer Datenschutzvereinbarung bearbeitet
- Die Aufträge werden nach den vereinbarten Dokumenten gemäß den Anweisungen des Kunden bearbeitet
- Es werden Prozesse für den Umgang mit Kundendaten im Hinblick auf Verfügbarkeit, Vertraulichkeit und Datenintegrität definiert.
- Die Kundendaten sind während der gesamten Bearbeitungszeit identifizierbar
- Der Kunde hat das Recht, die Verarbeitung stichprobenartig zu kontrollieren.
- Automatische Löschung der Daten nach 3 Monaten ab Dateneingang (sofern nicht anders angegeben)

3.7 Verwaltung von Verfügbarkeit und Ausfallsicherheit des Systems

Es wurden Maßnahmen ergriffen, um die Verfügbarkeit der Daten zu gewährleisten. Zu den bestehenden Maßnahmen gehören:

- Quellen für die unterbrechungsfreie Stromversorgung der IT-Infrastruktur
- Verwendung redundanter HW-Server und Firewall
- Mehrstufiger Sicherungsplan für Server und Stationen
- Überwachung der Verwendung der Lizenzen
- Definierter IT-Notfallplan

- Bereitstellung von externen IT-Dienstleistungen in Form von vertraglichen SLA-Konditionen
- Verwendung eines Antiviren-Systems
- Verwendung einer Firewall
- Klimatisierung von Serverräumen
- Gewährleistung des Brandschutzes in Gebäuden

3.8 Abteilung Systeme

- Einzelne LAN-Segmente werden durch VLANs getrennt
- Eine DMZ wird auf der Firewall definiert, um den Zugriff auf Daten zu trennen
- Die Daten werden physisch und logisch in getrennten Speichern oder Datenbanken getrennt aufbewahrt.
- Es gibt eine Trennung von Test- und Produktionsumgebung
- Die Tests werden auf logisch oder physisch getrennten Elementen durchgeführt (Datenbank, Virtualisierung, Sandbox)
- Verfahren für das Änderungsmanagement sind definiert

4 Liste der zugehörigen Dokumente

Id:	Titel des Dokuments:
Gesetz 110/2019 Slg.	§ 40 - Sicherheit der Verarbeitung personenbezogener Daten
Gesetz 110/2019 Slg.	§ 46 - Pflichten der Personen bei der Sicherung personenbezogener Daten
Verordnung (EU) 2016/679	Artikel 32 - Sicherheit der Verarbeitung
ISMS-DP-01	ISMS-Planung, -Betrieb und -Management
ISMS-DP02	Verschlüsselung der Daten

5 Liste der verwendeten Abkürzungen

GDPR – General Data Protection Regulation