Technisch-organisatorische Maßnahmen (TOMs) zur Datensicherheit

Dokumentation DO0020 - Rev.: 2.2

Inhaltsverzeichnis

1 Zielsetzung

Dieses Dokument beschreibt die technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO.

2 Geltungsbereich

Dieses Dokument gilt ab dem 01.05.2023 für alle deutschen Paragon-Standorte:

- Paragon Germany GmbH, Gutenbergstraße 3-5, 92421 Schwandorf
- Paragon Germany GmbH, Betriebsstätte Korschenbroich, Mühlenstraße 57, 41352 Korschenbroich
- Paragon Germany GmbH, Betriebsstätte Magdeburg, Marienstraße 1, 39112 Magdeburg
- Paragon Customer Communications Weingarten GmbH[1], Josef-Bayer-Straße 5, 88520 Weingarten

3 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Zutrittskontrolle

(Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, verwehrt wird)

[1] Wird voraussichtlich Ende 2023 mit der „Paragon Germany GmbH“ fusioniert.

- Alle Außentüren der Betriebsgebäude sind verschlossen. Ein Zutritt zu den Geschäftsräumen ist nur den zutrittsberechtigten Personen möglich, Dritten nur in Begleitung eines Mitarbeiters[2].
- Für die Vergabe von Berechtigungen an Mitarbeiter sind die Vorgesetzten zuständig. Die Einrichtung der Zutrittsberechtigungen und deren Entzug erfolgt zentral und revisionssicher durch die örtliche Personalsachbearbeitung oder durch das Facility Management.
- Es existieren Zutrittsregelungen für betriebsfremde Personen (z. B. Wartungs- und Reinigungspersonal, Besucher, Dienstleister). Diese und andere fremde Personen dürfen nur in Begleitung von berechtigten Mitarbeitern die Sicherheitsbereiche betreten. Jeder betriebsfremde Dritte wird in Schriftform auf den Datenschutz und zur Geheimhaltung verpflichtet, in Listen mit der Registrierung der Besucherausweisnummer, der besuchten Person und dem Zeitraum erfasst und erhält einen personalisierten Besucherausweis.
- Die Authentisierung der Zutrittsberechtigung erfolgt durch ein elektronisches Zutrittskontrollsystem. Die Zutrittsberechtigungen sind im System hinterlegt, werden über Token gesteuert und unterliegen einer regelmäßigen Prüfung.
- Der Zutritt zu den Serverräumen ist nur einem definierten und ausdrücklich berechtigten Personenkreis möglich. Zusätzlich wird der Zutritt durch eine Zwei-Faktor-Authentisierung geschützt. Alle Serverräume sind durch eine Alarmanalage gesichert.
- Es gibt für die Betriebsgebäude abgestufte Sicherheitszonen und damit verbunden dedizierte Zutrittsberechtigungen.
- Alle Zutritte werden protokolliert, sodass überprüft werden kann, wer zu welchem Zeitpunkt wo Zutritt hatte. Das Zutrittskonzept lässt es zu, den Zutritt für jeden Bereich und jeden Mitarbeiter im Detail (zeit- und personengebunden) zu regeln.
- Die Betriebsstätten werden außerhalb der Geschäftszeiten durch eine Alarmanlage gesichert. Die Alarmmeldungen gehen direkt an Sicherheitsunternehmen, die unmittelbar einen definierten Personenkreis informiert, der die weiteren, im Einzelfall gebotenen Maßnahmen definiert.
- Die Betriebsstätten sind zur Außenhautsicherung kameraüberwacht.
- Die Einhaltung der Zutrittsschutzmaßnahmen werden im Rahmen interner Audits und Regelkontrollgängen von Datenschutzkoordinatoren und vom Facility Management überwacht.

3.2 Zugangskontrolle

(Die Zugangskontrolle gewährleistet, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -verfahren gehindert werden.)

- Die PC-Arbeitsplätze sind zugangsgeschützt. Benutzer können auf gespeicherte Dateien nur zugreifen oder Daten nur speichern, sofern sie dafür über das Active Directory berechtigt sind.
- Die persönlichen Passwörter aller Mitarbeiter sind mindestens 12-stellig, und beinhalten mindestens Zeichentypen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen). Der Passwortwechsel wird nach spätestens 32 Tagen erzwungen. Nach fünfmaliger Falscheingabe wird das Benutzerkonto gesperrt und

[2] Der besseren Lesbarkeit wegen wird in diesem Dokument nur die männliche Form benutzt. Sie gilt für alle Geschlechter gleichermaßen.

kann nur durch einen Administrator wieder freigeschaltet werden. Das Mindestalter des Passwortes beträgt einen Tag und es darf für 13 Iterationen nicht wiederverwendet werden.

- Zur Anmeldung / Identifizierung im System muss der Benutzer seine UserID und sein persönliches Passwort eingeben. Im Active Directory sind die Zugangsberechtigungen hinterlegt, wobei der Zugriff auf die DV-Systeme selbst nur durch dafür berechtigte und autorisierte Personen erfolgen kann (Administratoren). Sämtliche Zugänge (erfolgreiche und abgewiesene) werden protokolliert.
- Der Internet-Zugang und das interne Netzwerk sind gegen ungewollte Zugriffe von außen durch den Einsatz von Next Generation Firewalls und mittels Netzwerksegmentierung abgeschottet.
- PC-Arbeitsplätze werden beim Verlassen gesperrt. Mittels zentraler Domain Policies ist festgelegt, dass die Sperre des Arbeitsplatz nach längerer Inaktivität des PC-Arbeitsplatzes automatisch erfolgt.

3.3 Zugriffskontrolle

(Die Zugriffskontrolle gewährleistet, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und diese nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.)

- Die Zugriffskontrolle erfolgt durch Benutzerkennungen und Passwörter. Ein Zugriff auf die Server ist nur mit gesonderter Authentifizierung der Benutzer möglich; es existieren getrennte Benutzerkonten für Administratortätigkeit und Sachbearbeitung. Jeder Mitarbeiter erhält nur die Berechtigungen, die für die Erfüllung seiner Tätigkeit notwendig sind. Die personenbezogene Authentifizierung erfolgt durch die Zugangskontrolle.
- Hinterlegte Notfallpassworte.

3.4 Trennungskontrolle

(Das Trennungsgebot gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.)

- Über den gesamten Produktionsprozess ist jederzeit gewährleistet, dass jeder Datensatz jedem Mandanten logisch zugeordnet werden kann.
- Getrennte Test- und Entwicklungsumgebung.
- Separate Jobs im Pre-Processing und der Produktion (bei der Produktion erfolgt dies durch die Bildung kundenbezogener Ausgabestapel, die separat verarbeitet werden).

3.5 Pseudonymisierung und Verschlüsselung

- Das Verfahren zur Verschlüsselung des Datenaustausches wird mit dem Kunden abgestimmt festgelegt.
- E-Mails werden bei Bedarf Ende-zu-Ende verschlüsselt.
- Datenträger von mobilen Endgeräten sind verschlüsselt

- Eine Pseudonymisierung der Daten muss vom Auftraggeber selbst durchgeführt werden, da nur der Eigentümer der Daten diese in geeigneter Form verändert darf. Nur mit der Zustimmung des Eigentümers kann der Auftragnehmer die Pseudonymisierung übernehmen (kostenpflichtig).

4 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Weitergabekontrolle

(Die Weitergabekontrolle gewährleistet, dass Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.)

- Für die abgesicherte Datenübermittlung zwischen Kunden und Auftragnehmer werden verschlüsselte Datenübertragungswege z. B. per sFTP oder VPN eingesetzt. Maßgebend ist die Kundenanforderung im Einzelfall, die ausdrücklich schriftlich erklärt werden muss.
- Die Datenlöschung im Bereich Print erfolgt automatisiert höchstens 30 bis 90 Tage nach Auftragsende - es sei denn, eine ausdrückliche Kundenanforderung bedingt eine abweichende Löschfrist.
- Die Verwendung von Massenspeichermedien an Laptops/PCs wird technisch reglementiert; Ausnahmen werden geprüft und das Ergebnis der Überprüfung dokumentiert.
- Es werden nur freigegebene Umgebungen für den Dateiaustausch mit externen Stellen verwendet und die dortige Übermittlung protokolliert. Maßgebend ist die Kundenvorgabe im Einzelfall.
- Zugriff aufs Firmennetzwerk nur mit firmeneigener Hardware erlaubt und bei mobiler Arbeit nur über VPN möglich
- Alle Datenübertragungen werden protokolliert. Bei Dateneingang wird die Datenübertragung auf ihre Vollständigkeit hin überprüft.
- Die Datenträgervernichtung erfolgt kontrolliert durch einen zugelassenen und zertifizierten Entsorger bzw. vor Ort durch eine Industrieschredderanlage.
- Die Datenübermittlung innerhalb der Produktionsstandorte erfolgt in gesicherten Bereichen der Paragon.

4.2 Eingabekontrolle

(Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.)

- Protokollierung der Datenaufbereitung (soweit Veränderungen am Content vertraglich vereinbart wurden).
- Definierte Aufbewahrungsfristen von Systemlogs/-ereignissen zu Nachweiszwecken.

5 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

5.1 Verfügbarkeitskontrolle

(Die Verfügbarkeitskontrolle gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

- Eine Notstromversorgung wichtiger IT-Systeme ist gewährleistet.
- Die Vorschriften zum Brandschutz werden beachtet und eingehalten, im Rahmen von Brandschutzbegehungen überprüft und die hier gemachten Auflagen umgesetzt. In allen Räumen herrscht Rauchverbot.
- Auf außerhalb der Arbeitszeiten geschlossene Fenster, gesicherte Türen und dem aufgeräumten Arbeitsplatz ist von allen Mitarbeitern zu achten. Jeder Mitarbeiter hat in seinem Bereich für die Sicherung des Arbeitsplatzes und des Gebäudes zu sorgen.
- Alle Bereiche wie Serverraum, Produktionsräume und Büros sind brandschutzgesichert mit Feuer- und Rauchmeldeanlagen sowie Feuerlöschgeräten. Es besteht eine Alarmaufschaltung zur Feuerwehr.
- Regelmäßige Sicherung der zur Verarbeitung der Daten erforderlichen Programme und Skripte.
- Klimatisierte und temperaturüberwachte Serverräume.
- Advanced Endpoint Protection.
- Kontinuierliche Lizenzüberwachung zur Vermeidung von Ausfällen systemkritischer Systeme.
- Ein Notfallhandbuch inklusive der zu ergreifenden Sofortmaßnahmen ist erstellt.

6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

6.1 Auftragskontrolle

(Die Auftragskontrolle gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.)

- Die Mitarbeiter werden regelmäßig im Bereich Datenschutz und Informationssicherheit geschult. Alle Mitarbeiter verpflichten sich vor Beginn der Auftragsverarbeitung auf unsere Geheimhaltungs-, Datenschutz- und Informationssicherheitsvorgaben, der Verpflichtungserklärung.
- Es besteht ein Verfahren zur Dienstleister- / Lieferantenauswahl und -bewertung. Lieferanten und Dienstleister sind zumindest einmal jährlich zu bewerten.
- Die mit der Auftragsbearbeitung befassten Mitarbeiter werden auf die Auftragsspezifikation des Auftraggebers hingewiesen. Das schließt die spezifizierten Arbeitsanweisungen mit ein.
- Sämtliche Verträge und Auftragsbestätigungen liegen vor und enthalten alle Pflichten, Aufgaben und Vorgaben von Auftraggeber und Auftragnehmer.

- Der Auftraggeber kann Personen/Stellen benennen, die Weisungen zu Aufträgen erteilen dürfen. Der Auftragnehmer verpflichtet sich dann, dass nur von diesen Personen/Stellen Weisungen entgegengenommen werden.

6.2 Managementsysteme

- Aktive Unterstützung von Datenschutzpolitik und Datenschutzzielen durch die Geschäftsführung
- Etabliertes Datenschutzmanagement-, ISO-9001-Qualitäts- und ISO-27001-Informationssicherheits-system
- Regelmäßige Überprüfung der technischen und organisatorischen Sicherheitsmaßnahmen
- Kontinuierlicher Verbesserungsprozess
- Datenschutz- und informationssicherheitsrelevante Richtlinien
- Kontinuierliche Datenschutz- und Informationssicherheitsschulungen der Mitarbeiter (eLearning, persönlich, Mitarbeiter-Zeitschrift)

Der Auftragnehmer gewährt dem Auftraggeber auf dessen Wunsch die Einsicht in sein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsdatenverarbeitung.

7 Mitgeltende Dokumente

- Leitlinie LL0014 „Datenschutzkonzept PCC DE“
- Formular FO0022 „Vertrag zur Auftragsverarbeitung für KBR-Kunden (AVV)“
- Formular FO0120 „Vertrag zur Auftragsverarbeitung für SAD-Kunden (AVV)“
- Formular FO0121 „Vertrag zur Auftragsverarbeitung für WGT-Kunden (AVV)“