Anlage 3 zum Datenschutzvertrag gemäß Art. 28 DSGVO

Technische und organisatorische Maßnahmen der LOROP GmbH

Informationen zum Dokument	
Version	01.04
Datum	28.03.2023
Dokumentenklassifikation	Öffentlich
Erstellt durch	Datenschutzbeauftragter LOROP GmbH
Genehmigungsstatus	Genehmigt
Genehmigt durch	Ronny Runge, Geschäftsführer LOROP GmbH
Freigegeben am	28.03.2023

Hinweis
Dieses Dokument enthält Informationen, welche Geschäftspartnern, Kunden sowie weiteren externen Stellen, die ein gesetzliches oder sonstig begründetes Einsichtsrecht haben, zur Verfügung gestellt werden.
Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige aller Geschlechter.

Präambel
Der Verantwortliche hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert.

1. Vertraulichkeit

Vertraulichkeit ist die Eigenschaft, dass personenbezogene Daten unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.

Zutrittskontrolle
Die Zutrittskontrolle soll einen unbefugten Zutritt verhindern, dabei bezieht sich der Begriff auf die räumliche Kontrolle.

Umgesetzte Maßnahmen
Empfangsbereich
Individuelle, dokumentierte und rollenabhängige Zutrittsberechtigungen (Transponder und/oder Schlüssel)
Begleitung der Besucher durch eigene Mitarbeiter
Unterbringung der Server in verschlossenen Räumen und/oder Serverschränken
Zutritt zum Rechenzentrum nur für eingeschränkten Personenkreis
Sicherung aller Räumlichkeiten auch außerhalb der Arbeitszeit

Zugangskontrolle
Verhinderung des Eindringens Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung.

Umgesetzte Maßnahmen
Formale Benutzer- und Berechtigungsverfahren
Prozess für Rechteanpassung und -entzug • beim Eintritt und Austritt von Mitarbeitern • bei Aufgabenänderung von Mitarbeitern
Verwendung von individuellen Passwörtern, auch initial
Passwort Policy mit Mindestvorgaben zur Passwortkomplexität: • Mindestens 8 Ziffern Zeichen / Groß- und Kleinschreibung, Sonderzeichen, Zahl • Verhinderung von Trivialpasswörtern • Passworthistorie (keine erneute Verwendung der letzten 5 Passwörter)
Login nur mit Benutzername, Passwort und wo erforderlich 2-Faktor-Authentifizierung
Bitlocker-Kennwort oder -PIN
Automatische Sperrung von Benutzerkonten nach mehrfacher Fehleingabe von Passwörtern
Anweisung, Bildschirmsperre bei Verlassen des Arbeitsplatzes manuell zu aktivieren
Clean Desk-Policy

Zugriffskontrolle
Unerlaubte Tätigkeiten in DV-Systemen, außerhalb eingeräumter Berechtigungen, sind zu verhindern.

Umgesetzte Maßnahmen
Umsetzung von Berechtigungskonzepten nach dem Need-to-Know-Prinzip
Trennung von Anwendungs- und Administrationszugängen
Protokollierung von Zugriffsversuchen
Minimale Anzahl an Administratoren
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen • lesen • schreiben • ausführen
Es werden die aufgelisteten Sicherheitssysteme (Software/Hardware) eingesetzt. • Virenscanner • Firewalls • SPAM-Filter • Intrusiondetection (IDS)
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)
Regelmäßige Auswertung von Log-Files
Absicherung der Datenbanken gegen unautorisierte Abfragen
Nutzung kryptografischer Verfahren (z.B. Verschlüsselung aller Endgeräte und Verschlüsselung bei Datenübertragung)
Alle IT-Systeme werden durch eine einheitliche Sicherheitslösung abgesichert.
Nutzung von Dokumentenvernichtung: Es stehen für die Vernichtung von Dokumenten in Papierform Shredder (Schutzklasse 2 / Sicherheitsstufe 4 (S2- P4)) nach DIN 66399 zur Verfügung. Datenträger (Festplatten, USB-Sticks, o.ä.) werden bis zur Vernichtung in einem Safe gelagert. Vernichtung erfolgt nach S2-H4, durch einen externen, zertifizierten Betrieb nach DIN 66399.

Pseudonymisierung
Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Umgesetzte Maßnahmen
Sofern möglich oder erforderlich werden personenbezogene Daten pseudonymisiert verarbeitet (Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System)

Trennungskontrolle
Daten, die zu unterschiedlichen Zwecken erhoben werden, sind getrennt zu verarbeiten.

Umgesetzte Maßnahmen
Trennung von Entwicklungs-, Test- und Produktivumgebung
Personenbezogene Daten dürfen nicht für Testzwecke verwendet werden
Mandantenfähigkeit / logische Trennung von Daten bei relevanten Anwendungen: Separate Datenbanken, Schema-Trennung in Datenbanken, Berechtigungskonzepte und/oder strukturierte Dateiablage
Berechtigungskonzept, das der getrennten Verarbeitung von Daten unterschiedlicher Kunden Rechnung trägt

2. Integrität

Die Integrität personenbezogener Daten ist dann gewahrt, wenn sie richtig, unverändert und vollständig sind.

Weitergabekontrolle
Bestehende Versendungsart zwischen Kunden, Auftraggebern und / oder Dritte.

Umgesetzte Maßnahmen
Bereitstellung von Daten über verschlüsselte Verbindungen
Weitergabe von personenbezogenen Daten im Sinne des Need-to-Know / Need-to-Do-Prinzips
Personenbezogene Daten werden nach ihrem Schutzbedarf klassifiziert, wobei vertrauliche Daten nur über sichere Kommunikationswege übertragen werden dürfen
Wo notwendig wird E-Mailverschlüsselung eingesetzt
Wo notwendig, werden personenbezogene Daten nur in pseudonymisierter oder anonymisierter Form übermittelt
Dokumentation der Weitergabe von physischen Speichermedien
Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag

Eingabekontrolle
Die Nachvollziehbarkeit durch Dokumentation der Datenverwaltung und -pflege.

Umgesetzte Maßnahmen
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
Rollenbasiertes Berechtigungskonzept (Lese-, Schreib-, und Löschrechte)
Protokollierung von administrativen Änderungen

3. Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

Die Verfügbarkeit von personenbezogenen Daten ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können

Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
Die Daten sind gegen Zerstörung und / oder Verlust geschützt.

Umgesetzte Maßnahmen
Einsatz von Hardware- und Softwarefirewalls
Intrusion Detection Systeme
Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag
aktuelle Datensicherungen
Datensicherungs- und Backupkonzepte
Regelmäßige Durchführung von Wiederherstellungstests
Regelmäßiger Test von Datensicherungen
Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt
Regelmäßige Sicherheitstests
Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten
Klimatisierte Serverräumlichkeiten
Serverraumüberwachung Temperatur und Feuchtigkeit
Rauchmelder
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)
USV-Anlage (Unterbrechungsfreie Stromversorgung)
Erfassung und Dokumentation von IT-Systemen
Serverräumlichkeiten in mehreren separaten Brandabschnitten
Einbeziehung des Einflusses angrenzender baulicher Einrichtungen in der Sicherheitsbeurteilung
Datenspeicherung auf RAID-Systemen
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)
Nach Prüfung der zur Verfügung stehenden Soft- und Firmwareupdates erfolgt die umgehende Installation. • Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden. • Definition von Zeiträumen, in denen die Updates implementiert werden sollen (z.B. Perioden niedrigerer Operationen, Wartungszeiten usw.). • Progressive Bereitstellung von Updates / Patches, um Probleme frühzeitig zu erkennen, ohne mehrere Geräte zu beeinträchtigen.
Regelmäßige Trainings- und Sensibilisierungsmaßnahmen innerhalb der Organisation • Datenschutz • E-Mailnotifikation über aktuelle Sicherheitsprobleme • Hardware

• Software • Kommunikation • Sicherheit
Identifikation aller IT-Geräte und der Infrastruktur
Erstellung einer Risikoanalyse über alle IT-Geräte, Infrastruktur und Vermögenswerte zur Ermittlung der Bedrohungen, inklusive ihrer Wahrscheinlichkeit und ihrer Auswirkungen.
Instandhaltung der Systeme entsprechend der Wartungsliste
Kapazitätsmessung
Sicherheit der Verkabelung (Datenleitung/ Stromleitung/ Telekommunikationsleitung)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der ergriffenen Datensicherheitsmaßnahmen.

Umgesetzte Maßnahmen
Regelmäßige interne Kontrolle der Sicherheitsmaßnahmen
Bei negativem Kontrollergebnis werden die Sicherheitsmaßnahmen angepasst und umgesetzt
Regelung der privaten Nutzung betrieblicher Mittel
Ausnahmeregelung der betrieblichen Nutzung privater Geräte (BYOD)
Regelung zur Nutzung von Datenträgern im betrieblichen Ablauf
Datenschutzbeauftragter ist benannt
Brandschutzbeauftragte sind benannt
Alle Mitarbeiter sind auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet
Mitarbeiter sind im Umgang mit personenbezogenen Daten sensibilisiert
Neue Mitarbeiter erhalten eine Onboarding-Schulung bezüglich des Umgangs mit personenbezogenen Daten
Ein Verzeichnis von Verarbeitungstätigkeiten wird gepflegt und Datenschutzfolgenabschätzungen werden bei Bedarf durchgeführt
Prozesse zur Wahrnehmung von Betroffenenrechten sind etabliert

Incident-Response-Prozess
Prozess zum Umgang mit Sicherheitsverletzungen und Systemstörungen, sowie zur Identifizierung, Eingrenzung, Beseitigung und Wiederherstellung.

Umgesetzte Maßnahmen
Dokumentierter Prozess zur Erkennung, Meldung und Dokumentation von Datenschutzverletzungen unter Einbindung des Datenschutzbeauftragten
Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

Datenschutzfreundliche Voreinstellungen
Es wird gewährleistet, dass durch datenschutzfreundliche Voreinstellungen nur Daten zweckbestimmt verarbeitet werden.

Umgesetzte Maßnahmen
Es wird prozessual sichergestellt, dass Systeme und Produkte datenschutzfreundlich entwickelt werden
Es werden nur diejenigen personenbezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind

Auftragskontrolle
Es wird sichergestellt, dass Daten die im Auftrag verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden. Gilt auch für Subunternehmen.

Umgesetzte Maßnahmen
Vertragsabschluss gem. gesetzlichen Vorgaben (Art. 28 DSGVO)
Daten die im Auftrag verarbeitet werden, werden nur nach Weisungen des Auftraggebers verarbeitet
Auftragnehmer werden im Hinblick auf getroffene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sorgfältig ausgewählt
Weisungen zum Umgang mit personenbezogenen Daten werden in Textform dokumentiert
Sofern erforderlich, werden Auftragsverarbeitungsvereinbarungen bzw. geeignete Garantien zur Übermittlung von Daten an Drittländer geschlossen
Vertragsmanagement - Erfassung vorhandener Dienstleister
Kontrolle vorhandener IT-Sicherheitszertifikate der Auftragnehmer
Auswahlprozess unter Berücksichtigung der gesetzlichen Vorgaben