Technische und organisatorische massnahmen Luware AG

Herausgegeben 01.01.2019

Luware Deutschland GmbH,
Schlossstrasse 70,
70174 Stuttgart,
Deutschland

solutions@luware.com
+49 711 8998 9621
www.luware.com

VERTRAULICHKEIT

- **Zutrittskontrolle:** Verhinderung des Zutritts Unbefugter zu Datenverarbeitungsanlagen

Sicherheitsschlösser, Chipkarten-/Transponder-Schliesssystem, Türsicherung (elektrischer Türschliesser, Fernsehmonitor), Alarmanlage, Einbruchsmeldesystem, Videoüberwachung, Besucher nur in Begleitung eines Mitarbeiters zugelassen, Nachprüfbare Schlüsselregelung, Schließung Bürotüren bei Abwesenheit / außerhalb der Arbeitszeit, Schließung Fenster bei Abwesenheit / außerhalb der Arbeitszeit, Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage, Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde), Fremdfirmen unter Aufsicht, Regelung für Firmenfremde (Besucherregelung), Sicherheitsbereiche

- **Zugangskontrolle:** Verhinderung unbefugter Systemnutzung

Einsatz von Verschlüsselungsroutinen für Dateien und Datenträger, Zugang zu kabellosem Netzwerk verschlüsselt (WLAN), Kontrollierte Vernichtung von Datenträgern, Kennwortrichtlinie, Clean-desk-policy, Sperre Benutzer bei wiederholt falscher Eingabe des Kennworts, Prozess bei Eintritt eines Mitarbeiters, Prozess bei Austritt eines Mitarbeiters, Arbeitsanweisung und Bearbeitungsverfahren für Datenerfassungsvorlagen, Prüf-, Abstimm- und Kontrollsysteme, Richtlinien für die Dateiorganisation (Anlage in Projektordnern/Shares/etc.), Automatische Sperre Bildschirm/Arbeitsplatz bei Abwesenheit, Vergabe und Sicherung von Identifizierungsschlüsseln, Verpflichtung auf das Datengeheimnis (alle Mitarbeiter unterzeichnen vor Aufnahme ihrer Tätigkeit bei Luware eine Geheimhaltungsvereinbarung), Einsatz von Benutzernamen / Passwörtern für Daten und Programme, Differenzierte Zugriffsregelung, Verschließbarkeit von Datenstationen, Einrichtung eines Benutzerstammsatzes pro User, Einsatz einer aktuellen Firewall, Einsatz eines aktuellen Virenschutzes, Funktionelle und/oder zeitlich beschränkte Nutzung von Endgeräten/Terminals, Identifizierung eines Endgerätes/Terminals am IT-System

- **Zugriffskontrolle**: Benutzerkontrolle; Unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems verhindern

Verschlüsselung von Laptops, Verwaltung der Benutzerrechte durch Systemadministratoren, Einsatz einer aktuellen Firewall, Videoüberwachung, Zeitliche Begrenzung der Zugriffsmöglichkeiten, Einsatz eines aktuellen Virenschutzes, Anzahl der Administratoren auf das Notwendigste reduziert (need-to-know Basis), Einsatz eines zusätzlichen Accounts ohne Administratorberechtigungen bei Administratoren, Überprüfung der Berechtigung, Beschränkung der freien Abfragemöglichkeiten von
Datenbanken (Query-Sprache), Einsatz von Aktenvernichtern, Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat), Datenschutzkonforme Löschung / Überschreibung vor Wiederverwendung von Datenträger, Einsatz von personifizierten Administrator-accounts, Einsatz von Verschlüsselungsroutinen für Dateien und Datenträgern, Prozess bei Eintritt eines Mitarbeiters, Prozess bei Austritt eines Mitarbeiters, Regelung der Zugriffsberechtigung (need-to-know Basis), Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen entsprechend der Aufgaben der Mitarbeiter, IT-Systemnutzung, Firewalls

- **Trennungskontrolle:** Getrennte Datenverarbeitung bei Daten, die zu unterschiedlichen Zwecken erhoben werden.

Getrennte Datenbanken, Separate Tabellen innerhalb von Datenbanken, Getrennte Ordnerstrukturen (Auftragsverarbeitung), Logisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern,

Mandantentrennung (Zweckbindung), Trennung von Netzen (physikalisch / logisch) nach Anwendung (Produktion/Test/DMZ), Trennung von Produktiv- und Testsystem

- **Pseudonymisierung:** Zum Zweck der Datenminimierung

Pseudonymisierung findet bei Luware wo sinnvoll und möglich auf Anfrage statt; die Verarbeitung der persönlichen Daten erfolgt dann auf eine Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.

INTEGRITÄT

- **Weitergabekontrolle / Übertragungskontrolle:** Verhindern von unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung

Einsatz einer aktuellen Firewall, Einsatz eines aktuellen Virenschutzes, Datenschutzkonforme Löschung / Überschreibung vor Wiederverwendung von Datenträger, Einsatz von Aktenvernichtern, Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat) inkl. Protokollierung der Vernichtung, Einsatz von Verschlüsselungsroutinen für Dateien und Datenträgern, Einsatz von VPNs, E-Mail-Verschlüsselung auf Anfrage, Festmontierte Plattenspeicher, Feststellung befugter Personen, Gesicherter Eingang Rechenzentrum für An- und Ablieferung, Gesonderter Verschluss vertraulicher Datenträger, Regelung der Anfertigung von Kopien, Sicherheitsschränke, Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

- **Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle:** Feststellung, ob und von wem persönliche Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt werden

Nachvollziehbarkeit/Protokollierung von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer, Einsatz elektronischer Signaturen, Verfahrens-, Programm- und Arbeitsablauforganisation, Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

VERFÜGBARKEIT / BELASTBARKEIT / WIEDERHERSTELLBARKEIT

Schutz gegen zufällige oder mutwillige Zerstörung oder Verlust

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort, Alarmmeldung bei unberechtigten Zutritten zu Serverräumen, Brandschutzmaßnahmen, Notfallplan, Backup- und Recoverykonzept, Virenschutzkonzept, Durchführung von regelmäßigen Backups, Ausgestaltung der Maßnahmen zur Objektsicherung, Feuer- und Rauchmeldeanlagen, Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen, Klimaanlage, Feuerlöschgeräte vor Serverräumen, Schutzsteckdosenleisten in Serverräumen, Serverräume nicht unter sanitären Anlagen / in der Nähe der zentralen Wasserversorgung, Spiegeln von Festplatten, z.B. RAID-Verfahren, Einsatz eines aktuellen Virenschutzes, Einsatz einer aktuellen Firewall, Service- und Wartungsverträge für Soft- und Hardware

REGELMÄSSIGE ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Datenschutz-Management Incident-Response-Management und Auftragsmanagement

Auftragsverarbeitung nur unter Weisung des Datenverantwortlichen (ADVs), Prüfung der Verfügbarkeit von erforderlichen Systemen, Datenträgern, Licensekeys etc. zur Sicherstellung der schnellen Wiederherstellbarkeit von Daten und Programmen (Desaster-Recovery-Szenarien), Regelmäßige Tests der Wiederherstellbarkeit von Daten und Programmen, Datenrücksicherungsszenarien: jeweilige Applikation muss auch im Versionsstand der Datensicherung vorliegen um Rücksicherung zu gewährleisten, Bestellung eines Datenschutzbeauftragten, Frühe Einbindung des Datenschutzbeauftragten in neue Projekte, Schaffung einer Datenschutzorganisation im Unternehmen, Datenschutzrichtlinien, Prozesse zur Optimierung des Datenschutzes, Regelmäßige Überprüfung der Datenschutzstandards, privacy by default, Verpflichtung auf das Datengeheimnis aller Mitarbeiter und sonstigen Dritten, Schulungen und Unterweisungen für Mitarbeiter, Zertifizierungen (insbesondere ISO 27001 wird Ende 2019 abgeschlossen sein)