Technische und organisatorische Maßnahmen der LAP GmbH zum Schutz von personenbezogenen Daten

Stand Januar 2024

Zutrittskontrolle: Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

- Berechtigungsausweise, elektronische Zutrittscodekarten/ Zutrittstransponder, Zutrittsberechtigungskonzept
- Alarmanlage
- Überwachung der Besucher
- Begrenzter und kontrollierter Zutritt zu Sicherheitsbereichen
- Gesondert gesicherter Zutritt zum Rechenzentrum
- Aufbewahrung der Server in verschlossenen Räumen, Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen
- Aufbewahrung der Daten-Backups

Zugangskontrolle: Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.

- Verschluss von Datenverarbeitungsanlagen und -geräten
- Passwortsicherung von Bildschirmarbeitsplätzen
- Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen
- Verwendung von individuellen Passwörtern
- Passwortpolicy mit Mindestvorgaben zur Passwortkomplexität
- Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
- Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern
- Prozess zum Rechteentzug bei Austritt von Mitarbeitern
- Verpflichtung der Mitarbeiter zur Vertraulichkeit (im Rahmen der gesetzlichen Vorschriften)
- Kontrollierte Vernichtung von Datenträgern

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

- Berechtigungskonzept
- Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)
- Regelmäßige Überprüfung von Berechtigungen
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken
- Regelmäßige Auswertung von Protokollen (Logfiles)
- Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)
- Einsatz von Sicherheitssystemen (Software/Hardware)
- Virenscanner
- Firewalls
- SPAM-Filter

Trennungskontrolle: Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Logische Datentrennung (z. B. auf Basis von Kunden- oder Mandantennummern)
- Berechtigungskonzept, das der getrennten Verarbeitung der Mandanten-Daten von Daten anderer Mandanten Rechnung trägt
- Rechte- und rollenbasiertes Zugriffskontrollsystem
- Trennung von Entwicklungs-, Test- und Produktivsystem

Weitergabekontrolle:

- Versand über VPN-Verbindung (IP-Sec)
- Keine Weitergabe ohne vorherige Vertraulichkeitsvereinbarung und nur wenn rechtlich zulässig
- Sichere Löschung von Datenträgern: Physikalische Zerstörung
- Papierentsorgung: Sicheres Vernichten von Papierdokumenten: Shredder gem. DIN 66399
- Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister gem. DIN 66399
- Möglichkeit der Fernsperrung oder Fernlöschung tragbarer Geräte

Eingabekontrolle: Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

- Festlegung von Benutzerberechtigungen (Profile)
- Differenzierte Benutzerberechtigungen: Lesen, Ändern, Löschen
- Feldzugriff bei Datenbanken
- Organisatorische Festlegung von Eingabezuständigkeiten
- Protokollierung von Eingaben/Löschungen (bei definierten Feldern)

Verfügbarkeitskontrolle: Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- Durchführung der Datensicherungs- und Backupkonzepte
- Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal
- Rauchmelder und Brandmeldeanlagen in Serverräumlichkeiten
- Klimatisierte Serverräumlichkeiten
- Blitz- / Überspannungsschutz
- Serverräumlichkeiten und Datenbackups in separaten Räumlichkeiten und Brandabschnitten
- Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitten

- Sicherstellung der technischen Lesbarkeit der Backup-Speichermedien für die Zukunft
- Katastrophen- oder Notfallplan (z. B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)
- USV-Anlage (Unterbrechungsfreie Stromversorgung)

Widerstandsfähigkeits- und Ausfallsicherheitskontrolle: Systeme müssen die Fähigkeit besitzen, mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

- Festplattenspiegelung
- Loadbalancer
- Datenspeicherung auf RAID-Systemen (RAID 1 und höher)
- Identifikation der verschiedenen Geräte, aus denen sich das Netzwerk zusammensetzt, und Bestimmung ihrer Hardware-Version sowie ihrer aktuellen Software- und Firmware-Versionen
- Externe Auftragnehmer und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist.
- Identifikation der IT-Geräte, Assets und Netzwerksysteme in der Infrastruktur der Organisation
- Kontrollverfahren: Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.
- Kontinuierliche interne Überwachung der Datensicherheitsmaßnahmen

Auftragskontrolle: Es ist sicherzustellen, dass Daten, die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden.

- Verträge mit Subauftragnehmern
- Bei Nutzung externer Server gewährleistet LAP, dass der Serveranbieter die hier beschriebenen Sicherheitsstandards erfüllen.

Ergänzende Regelungen für Fernzugang:

- Mitarbeiter, die Fernwartungen durchführen, sind zur Vertraulichkeit verpflichtet
- Fernwartungen erfolgen nur in Abstimmung und mit Zustimmung des Auftraggebers
- Der Auftraggeber hat die Möglichkeit, die Fernwartung zu kontrollieren und jederzeit zu unterbrechen
- Fernwartungen werden nur durch LAP-Personal durchgeführt
- Fernwartungen erfolgen ausschließlich aus dem entsprechenden LAP-Standort bzw. aus Deutschland heraus
- Des Weiteren gelten die technischen und organisatorischen Maßnahmen des Auftraggebers zum Schutz seiner Daten. Der Auftraggeber hat sicherzustellen, dass bei einer Fernwartung ein Zugriff von personenbezogenen Daten auf das erforderliche Minimum reduziert wird und kein Zugriff auf Daten möglich ist, die nicht Gegenstand der Fernwartung sind.

Zusätzliche Regelungen für die Verarbeitung von Patientendaten

HINWEIS: LAP ist nicht für die Verfügbarkeit von Patientendaten verantwortlich. LAP erhält Patientendaten ausschließlich für Support- und Servicezwecke und löscht die Patientendaten danach. Die Verfügbarkeit von Patientendaten liegt stets in der alleinigen Verantwortung des Auftraggebers.

- LAP kann im Fall von Support- oder Serviceleistungen Zugang zu Patientendaten haben oder Patientendaten erhalten
- Patientendaten werden nur verarbeitet, wenn LAP vom Kunden dazu angewiesen wird
- LAP arbeitet nach Möglichkeit nur mit anonymisierten Daten
- LAP-Mitarbeiter werden im Umgang mit Patientendaten geschult
- Zugang zu / Übermittlung von Patientendaten an LAP nur mit Genehmigung des Kunden
- Übermittlung von Patientendaten nur über eine separate gesicherte Uploadmöglichkeit
- LAP stellt für das Hochladen von Patientendaten bei Bedarf ein Extranet (B2B) über SharePoint zur Verfügung.
- Der Zugang zum Extranet erfolgt nur nach vorheriger Registrierung und mit begrenzten Zugangsrechten
- Kein Versand von E-Mails mit Patientendaten, E-Mails mit Patientendaten können blockiert werden
- Patientendaten werden getrennt von anderen LAP-Daten in verschlossenen Containern aufbewahrt
- Passwortschutz für Speichermedien mit Patientendaten
- Patientendaten, die auf Produkten gespeichert sind, die an LAP zur Wartung, Reparatur, Rückgabe oder zum Austausch gesendet werden, werden von LAP gelöscht.
- Begrenzte Zugriffsrechte auf Patientendaten (Need-to-Know / zeitlich begrenzt)
- Löschung der Patientendaten, sobald diese nicht mehr erforderlich sind

Lüneburg, Januar 2024

L A P GMBH LASER APPLIKATIONEN
Zeppelinstr. 23
21337 Lüneburg
Deutschland

Amtsgericht Lüneburg HRB 206423