TOM - technische und organisatorische Maßnahmen
lunchlist GmbH

Erstellungsdatum: 01.01.2024

Inhaltsverzeichnis

1. Pseudonymisierung und Verschlüsselung personenbezogener Daten (i.S.d. Art. 32 DSGVO)

Technische Maßnahmen:

Ende-zu-Ende-Verschlüsselung:
Implementierung einer Ende-zu-Ende-Verschlüsselung, um sicherzustellen, dass personenbezogene Daten während der Übertragung zwischen dem Benutzer und der Website geschützt sind.

Tokenisierung:
Partielle Verwendung von Tokenisierung für sensible Daten, um die tatsächlichen Daten durch generierte Token zu ersetzen, wodurch die Identifikation der Benutzer erschwert wird.

Organisatorische Maßnahmen:

Zugriffskontrolle und Berechtigungsmanagement:
Einführung strikter Zugriffskontrollen und regelmäßige Überprüfung von Berechtigungen, um sicherzustellen, dass nur autorisierte Personen Zugriff auf unverschlüsselte Daten haben.

Notfallwiederherstellungsplan:
Entwicklung eines Notfallwiederherstellungsplans für die Wiederherstellung der relevanten Daten.

Regelmäßige Überprüfungen:
Durchführung von regelmäßigen Überprüfungen, um sicherzustellen, dass die implementierten technischen Maßnahmen korrekt funktionieren und den Anforderungen der DSGVO entsprechen.

Datenschutz-Folgenabschätzung:
Durchführung von Datenschutz-Folgenabschätzungen, insbesondere wenn neue Verarbeitungsvorgänge eingeführt werden, um potenzielle Risiken zu identifizieren und zu adressieren.

2. Vertraulichkeit (i.S.d. Art. 32 DSGVO)

Technische Maßnahmen:

Verschlüsselung:
Einsatz von Transport Layer Security (TLS) oder Secure Sockets Layer (SSL) für die sichere Übertragung von Daten zwischen dem Endgerät des Benutzers und der Website.

Authentifizierung und Autorisierung:
Implementierung von Authentifizierungsmethoden (u. a. 2-Faktor-Authentifizierung) und klaren Autorisierungsrichtlinien (sog. Berechtigungskonzept innerhalb der lunchlist®), um sicherzustellen, dass nur berechtigte Benutzer auf sensible Daten zugreifen können.

Session-Management:
Sicheres Session-Management, um sicherzustellen, dass Sitzungen nach einer angemessenen Zeit automatisch ablaufen und um mögliche Session-Hijacking-Angriffe zu verhindern.

Sicherheitsupdates und Patch-Management:
Regelmäßige Aktualisierung von Betriebssystemen, Webservern, Datenbanken und anderen Softwarekomponenten, um bekannte Sicherheitslücken zu schließen.

Monitoring und Intrusion Detection:
Providerseitige Bereitstellung von Überwachungssystemen, um verdächtige Aktivitäten zu erkennen, sowie Intrusion Detection Systeme, um auf mögliche Angriffe zu reagieren.

Datensparsamkeit:
Implementierung von Mechanismen zur Datensparsamkeit, um sicherzustellen, dass nur kurzzeitig Daten für den jeweiligen Verarbeitungszweck verarbeitet werden.

Organisatorische Maßnahmen:

Sicherheitsrichtlinien und Schulungen:
Erstellung und Implementierung von klaren Sicherheitsrichtlinien sowie regelmäßige Schulungen für Mitarbeiter, um ein Bewusstsein für Datenschutz und Vertraulichkeit zu schaffen.

Zugriffskontrollen und Rollenmanagement:
Klare Festlegung von Zugriffsrechten und regelmäßige Überprüfung dieser Rechte, um sicherzustellen, dass nur autorisierte Personen auf sensible Daten zugreifen können.

Notfallplan und Incident Response:
Erstellung eines Notfallplans und einer Incident-Response-Strategie, um im Falle eines Sicherheitsvorfalls angemessen reagieren zu können.

Verträge mit Dienstleistern:
Klare Vereinbarungen mit Dienstleistern hinsichtlich der Vertraulichkeit von Daten und Sicherheitsanforderungen.

3. Integrität (i.S.d. Art. 32 DSGVO)

Technische Maßnahmen:

Hash-Algorithmen:
Verwendung starker kryptographischer Hash-Algorithmen, um die Integrität von gespeicherten Daten sicherzustellen.

Versionierung von Daten:
Implementierung einer Datenversionierung, um relevante Änderungen nachverfolgen und bei Bedarf wiederherstellen zu können.

Transaktionsprotokolle:
Einrichtung von Protokollen für relevante Transaktionen und Datenänderungen, um nachvollziehen zu können, wer, wann und welche Änderungen vorgenommen hat.

Zugriffskontrolle:
Implementierung von Zugriffskontrollen, um sicherzustellen, dass nur autorisierte Benutzer Änderungen an den Daten vornehmen können.

Verschlüsselung:
Verwendung von Verschlüsselungstechnologien, um sicherzustellen, dass Daten während der Übertragung und Speicherung vor Manipulation geschützt sind.

Organisatorische Maßnahmen:

Datenschutzrichtlinien:
Festlegung klarer Datenschutzrichtlinien und -verfahren, die den Umgang mit Datenänderungen und die Verantwortlichkeiten der Mitarbeiter regeln.

Zugriffskontrollrichtlinien:
Entwicklung von Zugriffskontrollrichtlinien, die den Grundsätzen der minimalen Berechtigungen folgen und sicherstellen, dass Mitarbeiter nur auf die Daten zugreifen können, die für ihre Aufgaben erforderlich sind.

Change-Management-Prozesse:
Implementierung von Change-Management-Prozessen, um sicherzustellen, dass Änderungen an der lunchlist® und den damit verbundenen Daten ordnungsgemäß dokumentiert, überprüft und genehmigt werden.

Incident-Prevention:
Überwachungssystems unseres Hosting-Providers um potenziellen Sicherheitsvorfällen vorzubeugen.

Dokumentation:
Führung von Aufzeichnungen über Datenänderungen an der lunchlist® und interne Überprüfungen, um die Einhaltung der Integritätsanforderungen zu überprüfen.

Notfallwiederherstellung:
Erstellung eines Notfallwiederherstellungsplans, um im Falle von Datenverlusten oder Manipulationen schnell wiederherstellen zu können.

4. Verfügbarkeit und Belastbarkeit (i.S.d. Art. 32 DSGVO)

Technische Maßnahmen:

Regelmäßige Backups:
Durchführung regelmäßiger Backups von Daten und Systemkonfigurationen, um im Falle eines Ausfalls schnell wiederherstellen zu können.

Monitoring und Alarme:
Implementierung von Überwachungssystemen durch unseren Hosting-Provider, um den Zustand der Infrastruktur kontinuierlich zu überwachen, und Einrichtung von Alarmen für ungewöhnliche Aktivitäten oder Leistungsprobleme.

Notfallwiederherstellungsplan (Disaster Recovery):
Erstellung und regelmäßige Aktualisierung eines Notfallwiederherstellungsplans, der klare Schritte für die Wiederherstellung des Betriebs nach einem Ausfall festlegt.

Distributed Denial of Service (DDoS)-Schutz:
Implementierung von DDoS-Schutzmechanismen, um Angriffe abzuwehren und die Verfügbarkeit der Website sicherzustellen.

Skalierung der Systemlandschaft:
Kontinuierliche Überprüfung der Systemressourcen, um eine optimale Leistung sicherzustellen.

Organisatorische Maßnahmen:

Service Level Agreements (SLAs):
Festlegung von klaren Service Level Agreements mit unserem Hosting-Provider und allen relevanten Dienstleistern, um Verfügbarkeitsanforderungen zu definieren.

Regelmäßige Wartung und Updates:
Durchführung regelmäßiger Wartungsarbeiten, um sicherzustellen, dass alle Systeme auf dem neuesten Stand sind und potenzielle Schwachstellen behoben werden.

Incident Response Plan:
Erstellung eines Incident Response Plans, der klare Verfahren für den Umgang mit Sicherheitsvorfällen und Ausfällen enthält.

Schulungen für das Supportteam:
Schulung des Supportteams, um schnelle und effiziente Reaktionen auf Supportanfragen im Zusammenhang mit Verfügbarkeitsproblemen zu gewährleisten.

Vertragsmanagement:
Überprüfung von Verträgen mit Dienstleistern hinsichtlich Verfügbarkeitsanforderungen.

5. Wiederherstellung der Verfügbarkeit und Zugänglichkeit personenbezogener Daten bei einem physischen oder technischen Zwischenfall (i.S.d. Art. 32 DSGVO)

Technische Maßnahmen:

Regelmäßige Backups:
Implementierung eines robusten Backup-Systems, das regelmäßig und automatisch personenbezogene Daten sichert.

Notfallwiederherstellungsplan (Disaster Recovery):
Entwicklung eines detaillierten Notfallwiederherstellungsplans, der Schritte für die Wiederherstellung der Daten und Dienste nach einem Zwischenfall festlegt.

Verteilte Backups:
Speicherung von Backups in separatem Brandabschnitt, um das Risiko lokaler Zwischenfälle zu verringern.

Testen von Wiederherstellungsprozessen:
Regelmäßige Tests der Wiederherstellungsprozesse, um sicherzustellen, dass im Ernstfall eine schnelle und effektive Wiederherstellung möglich ist.

Organisatorische Maßnahmen:

Schulungen und Bewusstseinsbildung:
Schulung von Mitarbeitern in Bezug auf den Notfallwiederherstellungsplan und Sensibilisierung für die Bedeutung einer schnellen Reaktion.

Kommunikationsplan:
Erstellung eines klaren Kommunikationsplans, der sicherstellt, dass alle relevanten Stakeholder effektiv über den Zwischenfall und die Wiederherstellungsmaßnahmen informiert werden.

Eskalationsverfahren:
Festlegung klarer Eskalationsverfahren, um sicherzustellen, dass bei einem Zwischenfall schnell die erforderlichen Entscheidungen getroffen werden können.

Regelmäßige Überprüfung und Aktualisierung:
Regelmäßige Überprüfung und Aktualisierung des Notfallwiederherstellungsplans im Einklang mit Änderungen in der Infrastruktur oder Geschäftsanforderungen.

Dokumentation von Zwischenfällen:
Evaluierung von Zwischenfällen und daraus gezogenen Lehren, um den Notfallwiederherstellungsplan kontinuierlich zu verbessern.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (i.S.d. Art. 32 DSGVO)

Technische Maßnahmen:

Penetrationstests:
Durchführung von Penetrationstests, um die Widerstandsfähigkeit der Systeme gegenüber Angriffen zu überprüfen und Schwachstellen zu beheben.

Intrusion Alarm System:
Bereitstellung eines Intrusion Alarm Systems durch unseren Hosting-Provider, um verdächtige Aktivitäten zu erkennen und darauf zu reagieren. Dies dient dazu, um das Risiko von Sicherheitsverletzungen zu minimieren.

Protokollierung:
Umfassende Protokollierung von Systemaktivitäten und regelmäßige Überprüfung der Protokolle, um ungewöhnliche Aktivitäten zu erkennen und aufzuzeichnen.

Organisatorische Maßnahmen:

Überprüfung von Zugriffsberechtigungen:
Regelmäßige Überprüfung der Zugriffsberechtigungen von Mitarbeitern und Dritten, um sicherzustellen, dass nur autorisierte Personen auf personenbezogene Daten zugreifen können.

Bewertung von Lieferanten und Dienstleistern:
Regelmäßige Bewertung der Sicherheitsmaßnahmen von Lieferanten und Dienstleistern, um sicherzustellen, dass sie den erforderlichen Datenschutzstandards entsprechen.

Mitarbeiterschulungen:
Regelmäßige Schulungen für Mitarbeiter, um sicherzustellen, dass sie über aktuelle Sicherheitsrichtlinien und -verfahren informiert sind.

Berichterstattung und Eskalationsverfahren:
Einführung klarer Berichterstattungsmechanismen und Eskalationsverfahren für Sicherheitsvorfälle, um eine schnelle Reaktion zu ermöglichen.

Dokumentation und Aktualisierung von Sicherheitsrichtlinien:
Dokumentation von Sicherheitsrichtlinien und regelmäßige Aktualisierung, um sicherzustellen, dass sie den aktuellen Bedrohungen und Anforderungen entsprechen.

Kontinuierliche Verbesserung:
Etablierung eines Prozesses für kontinuierliche Verbesserung der Sicherheitsmaßnahmen basierend auf den Ergebnissen von Überprüfungen und Evaluierungen.