Anlage **Technische und organisatorische Maßnahmen (TOM)** – nach § 9 BDSG bzw. Art. 32 DS-GVO.

nexato

Die Nexato GmbH sichert als Auftragnehmer gem. § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG bzw. Art. 32 DS-GVO allen Kunden folgende technische und organisatorische Maßnahmen (TOM) zur Wahrung der Datenschutzbestimmungen gem. DS-GVO zu. Dabei sind derartige Maßnahmen definiert, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

Paragraphen	Klartext
A. Vertraulichkeit	
1. Zutrittskontrolle	
Technische Maßnahmen Manuelle Schließsysteme; Sicherheitsschlösser	Auch, wenn unsere Daten maßgeblich bei Cloud-Dienstleistern gespeichert und verarbeitet werden, und wir keine eigenen Server in unseren Räumlichkeiten betreiben, haben wir Sicherheitsmaßnahmen vorgesehen, um Unbefugten keinen Zutritt zu gewähren und damit unberechtigte Einblicke auf jegliche Daten zu unterbinden.
Organisatorische Maßnahmen Schlüsselregelung (kontrollierte Schlüsselvergabe); Besucher nur in Begleitung von Mitarbeitern; Sorgfalt bei der Auswahl der Reinigungsdienste;	
2. Zugangskontrolle	
Technische Maßnahmen Interner Prozess zur Beantragung per E-Mail; Genehmigung von Benutzeraccounts/ -zugängen durch Geschäftsführung; Logins mit Benutzernamen und turnusmäßig erzwungenem Wechsel, der durch die Benutzer zu definierenden Passwörter gem. Richtlinien (Mindestlänge, Passworthistorie); Multifaktor-Authentifizierung; Einsatz Antiviren-Software; Verschlüsselung	Die Nutzung unserer Systeme oder Services ist ohne persönliche Zugangsdaten ausgeschlossen. Niemand – auch nicht unsere Mitarbeiter – haben unmittelbaren Zugriff auf ihre Daten. Grundsätzlich vergeben wir nur solche Benutzerrechte (ggf. temporäre Rechte), die unbedingt für die Arbeit unserer Mitarbeiter erforderlich sind und protokollieren jeden Vorgang. Informationen, die wir zum Beispiel für unsere

Paragraphen

Klartext

von Datenträgern und Speicher mobiler Geräte; regelmäßige Prüfung und Löschung von Zugängen/Accounts bei Unternehmensaustritt oder Funktionswechsel; verschlüsselte Speicherung von Passwörtern; Sperrung von Zugängen bei mehrfacher Fehleingabe;

Organisatorische Maßnahmen

Verwaltung von Benutzerberechtigungen; Erstellung von Benutzerprofilen; Richtlinien Active-Directory (AD); Dokumentation Benutzerrechte-Historie im AD; Benachrichtigung und Freigaberichtlinie bei Accountsperrung über Administrator; es werden nur so viele Zugänge wie notwendig erstellt: wer keinen Zugriff benötigt, wird nicht autorisiert und wer Zugänge erhält, wird vor der Freigabe auf Tauglichkeit im Umgang mit den zum Zugriff berechtigten Daten geprüft; Mitarbeiter sind zur Geheimhaltung jeglicher Passwörter und Daten angewiesen; turnusmäßige Schulung/ Einweisung der Mitarbeiter;

Entwicklungsprozesse benötigen, beinhalten – soweit möglich – keine persönlichen oder wenn dann weitestgehend pseudonymisierte Daten.

Unsere Mitarbeiter werden regelmäßig für den Umgang mit sensiblen Daten geschult und erhalten ausschließlich Zugriff auf für ihre Arbeit relevante Daten.

3. Zugriffskontrolle

Technische Maßnahmen

Monitoring und Protokollierung von Zugriffen auf Anwendungen, konkrete Eingaben, Änderungen und Löschung von Daten;

Wir haben jederzeit ein Auge darauf, wer, wann, wie, wo Zugriff auf welche Daten hat und was mit diesen Daten passiert.

Paragraphen

Organisatorische Maßnahmen

Einsatz Berechtigungskonzepte; minimale Anzahl an Administratoren; Verwaltung von Benutzerrechten durch Administratoren; 4-Augen-Prinzip; Genehmigungsrichtlinien inkl. Antragsverfahren und Dokumentation;

4. Trennungskontrolle

Technische Maßnahmen

Trennung von Produktiv- und Testumgebung; Mandantenfähigkeit relevanter Anwendungen; Sandboxing;

Organisatorische Maßnahmen

Steuerung über Berechtigungskonzept; Festlegung von Datenbank- und Zugriffsrechten; Datensätze sind mit Zweckattributen versehen;

5. Pseudonymisierung

Technische Maßnahmen

Im Falle der Pseudonomysierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (verschlüsselt); nicht notwendige, personenbezogene Daten werden vor dem Wegschreiben ins Log entfernt;

Klartext

Wir stellen eine getrennte Verarbeitung von Daten sicher, die zu unterschiedlichen Zwecken erhoben werden.

Wir gewährleisten, dass ein Datenexport vertraulicher Daten niemals möglich ist. Sollten wir doch irgendwann einmal personenbezogene Daten verarbeiten, werden wir diese Daten durch algorithmische Maßnahmen so anonymisieren, dass aus den Daten keine natürliche Person erkennbar ist.

Paragraphen

Organisatorische Maßnahmen

Interne Anweisung, personenbezogene Daten, im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist, möglichst zu anonymisieren/pseudonymisieren;

B. Integrität

6. Weitergabekontrolle

Technische Maßnahmen

Protokollierung von Zugriffen und Abrufen; Bereitstellung über verschlüsselte Verbindungen wie sftp, https, ssh, ssl; verschlüsselte Datenspeicherung (Encryption at Rest); Zugriffs- und Downloadberechtigungen (z. B. via Passwortschutz) inkl. Ablaufdaten für geteilte Ordner/Dokumente;

Organisatorische Maßnahmen

Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen (Audittrails); Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen;

Klartext

Die Datenintegrität stellen wir sicher, indem wir stets mit starker Verschlüsselung arbeiten und eine ungewollte Veränderung von Daten über die Anwendung von Prüfsummen umgehend identifizieren. Das Erstellen neuer oder Ändern bestehender Daten protokollieren wir für die bessere Nachvollziehbarkeit. Wir können also erkennen, wer wann was gemacht hat.

Paragraphen

Klartext

7. Eingabekontrolle

Technische Maßnahmen

Technische Protokollierung der Eingabe, Änderung und Löschung von Daten; manuelle oder automatisierte Kontrolle der Protokolle (Audittrails);

Organisatorische Maßnahmen

Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können; Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen; Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis des Berechtigungskonzepts; Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitung übernommen wurden; klare Zuständigkeiten für Löschungen;

Um jederzeit überprüfen zu können, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder gelöscht worden sind, protokollieren und überprüfen wir dererlei Zugriffe.

C. Verfügbarkeit und Belastbarkeit

8. Verfügbarkeitskontrolle

Technische Maßnahmen

Hosting in hochverfügbaren Rechenzentren; Verfügbarkeitsgarantien der eingesetzten Dienstleister gemäß Leistungsvereinbarung inkl. TOM; Backup der Datenbanken in anderen Verfügbarkeitszonen; Spiegelung der Anwen-

Wir überwachen alle unsere Dienste und tun alles in unserer Macht stehende für die höchstmögliche Verfügbarkeit und höchstmögliche Sicherheit. Wir üben regelmäßig verschiedene Ereignisse, um uns auf eine große Störung vorzubereiten und um dann sofort zu wissen, was wir tun müssen.

Paragraphen

dungskoten in andere Verfügbarkeitszonen; automatisierter Fail-Over im Problemfall; redundante Systemauslegung hinter Loadbalancern zum Schutz vor DDoS-Attacken;

Organisatorische Maßnahmen

Backup- und Recovery-Konzept; Kontrolle des Sicherungsvorgangs; regelmäßige Tests zur Datenwiederherstellung; regelmäßige Durchführung von Load-Tests;

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

9. Datenschutzmaßnahmen

Technische Maßnahmen

Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf und Berechtigung; dokumentiertes Sicherheitskonzept; regelmäßige Software-Tests; eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens jährlich durchgeführt;

Organisatorische Maßnahmen

Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis per Arbeitsvertrag verpflichtet; Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich; Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt;

Klartext

Wir stellen jederzeit einen sehr guten Datenschutz sicher und sorgen für einen datenschutzfreundlichen Betrieb. Niemals führen wir ohne deinen Auftrag eine Verarbeitung deiner vertraulichen oder persönlichen Daten durch. Außerdem gewährleisten wir, dass 24/7 erfahrene Mitarbeiter den Betrieb unserer Services sicherstellen.

Paragraphen

die Organisation kommt den Informationspflichten nach Art. 13 und 14 DS GVO nach; Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden; regelmäßige interne Sicherheitsauditierung;

10. Incident-Response-Management

Technische Maßnahmen

Einsatz von Firewalls und regelmäßige Updates; Einsatz von Spam-Filtern und regelmäßige Updates; Einsatz von Virenscannern und regelmäßige Updates; Intrusion Detection System (IDS); Intrusion Prevention System (IPS);

Organisatorische Maßnahmen

Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörden); Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen; Einbindung von externen Datenschutzexperten bei Sicherheitsvorfällen und Datenpannen; Dokumentation von Sicherheitsvorfällen und Datenpannen; Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen;

Klartext

Um potenzielle Risiken von vornherein zu reduzieren, setzen wir in allen Bereichen stets auf aktuelle Virenscanner, Firewalls, Spam-Filter sowie Sicherheitsfunktionen unserer Dienstleister.

Sollte es am Ende doch einmal zu einem Vorfall kommen, haben wir uns bereits im Vornherein einen klaren Plan gemacht, was zu tun ist, um die Sicherheit aller Daten schnellstmöglich wieder sicherzustellen bzw. Schadensbegrenzung vorzunehmen und rechtskonform zu agieren.

Paragraphen

11. Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind; einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen; soweit möglich Verarbeitung personenbezogener Daten ausschließlich in Staaten der europäischen Union (EU);

12. Auftragskontrolle (Outsourcing)

Organisatorische Maßnahmen

Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation; Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere in Bezug auf Datenschutz und Datensicherheit); Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln; falls erforderlich, schriftliche Weisungen an den Auftragnehmer; Verpflichtung zur Einhaltung der DS-GVO; Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer; Regelung zum Einsatz weiterer Subunternehmer; Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags; bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Klartext

Um unsere Services datenschutzkonform anbieten zu können, setzen wir bei der Verarbeitung von personenbezogenen Daten – soweit möglich – ausschließlich auf Subdienstleister, die EU-Recht unterstehen und den DS-GVO der europäischen Union Rechnung tragen.

Hierbei achten wir bereits bei der Auswahl darauf, dass diese Dienstleister unseren hohen Anforderungen an den Umgang mit sensiblen Daten entsprechen. Falls notwendig klären wir relevante Themen ab und treffen individuelle Vereinbarungen im Sinne unserer Kunden.