Datenschutzkonzept

Beschreibung der technisch-organisatorischen Sicherheitsmaßnahmen

Die Firma tetrateam trifft als Verantwortliche folgende technisch-organisatorische Maßnahmen, um die Sicherheits- und Schutzanforderungen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

1	**Vertraulichkeit**
Die Sicherstellung der Vertraulichkeit von Daten ist eine der wesentlichen Schutzziele der DSGVO. Maßnahmen zur Umsetzung des Gebots der Vertraulichkeit sind unter anderem Zutritts-, Zugangs- oder Zugriffskontrollen. Die in diesem Zusammenhang getroffenen technischen und organisatorischen Maßnahmen sollen eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, insbesondere des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung.	
Unsere Maßnahmen zur Sicherstellung der Vertraulichkeit:	
☐	Vertraulichkeitsvereinbarungen mit internen und externen Mitarbeiter*innen
☐	Vertraulichkeitsvereinbarungen mit externen Dienstleister*innen
☐	Festlegung und Kontrolle der Nutzung zugelassener Ressourcen bzw. Kommunikationskanäle
☐	Schutz vor äußeren Einflüssen durch Antivirensoftware (Programm-, Geräte- und Webkontrolle)
☐	Berücksichtigung der Grundsätze des Datenschutzes durch Technik und der datenschutzfreundlichen Grundeinstellungen – beispielsweise bei Kontaktformularen (Privacy by Design, Privacy by Default)
☐	Sorgfältige Auswahl der Personalkräfte hinsichtlich Fachlichkeit, geordneter Lebens- und Vermögensverhältnisse und Zuverlässigkeit sowie möglicher Interessenskonflikte
☐	Schutzbedarfsklassifizierung von personenbezogenen Daten
☐	Zutrittskontrolle (siehe Ziffer 1.1.)
☐	Zugangskontrolle (siehe Ziffer 1.2.)
☐	Zugriffskontrolle (siehe Ziffer 1.3.)
☐	Einsatz von Verschlüsselungsmechanismen (siehe Ziffer 1.4.)
☐	Trennungskontrolle (siehe Ziffer 1.5.)

1.1.	**Zutrittskontrolle**
Damit sind Maßnahmen gemeint, die Unbefugten den Zutritt zu den Büroräumen verwehren, in denen personenbezogene Daten verarbeitet werden.	
Unsere Maßnahmen zur Verwehrung des Zutritts zu Datenverarbeitungsanlagen für Unbefugte:	
☐	Festlegung raumspezifischer Zutrittsberechtigungen

☐	Zutrittsregelung / Vertraulichkeitsvereinbarungen unter Büronutzer*innen und mit externen Dienstleistern
☐	Restriktive Schlüsselregelungen / Sicherheitsschlösser
☐	Besucheraufenthalte in Räumen mit Rechnern nur in Begleitung von Berater*innen
☐	Besondere Sicherung nicht straßenseitig einsehbarer Fensterbereiche
☐	Nachbarschaftliche Vereinbarung zur Meldung verdächtiger bzw. problematischer Ereignisse
☐	Datensicherungen auf portablen Sicherungsmedien (z.B. externe Laufwerke) sind verschlüsselt und zusätzlich zutrittsgesichert

1.2.	**Zugangskontrolle**
Damit sind Maßnahmen gemeint, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und –verfahren benutzen. Hierzu gehören bspw. geeignete Passwortregeln.	
Unsere Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungssysteme nutzen:	
☐	Die Zugänge zu den Datenverarbeitungssystemen sind durch Benutzername und Passwort geschützt
☐	Die Passworte für die Datenverarbeitungssysteme haben eine Mindestkomplexität (Sonderzeichen, Zahlen & Ziffern, Groß & klein, Anzahl der Zeichen)
☐	Verbot der externen Weitergabe von Benutzernamen und Passworten
☐	Verschlüsselung aller gespeicherten Passwort-Daten
☐	Automatische Sperrung des Bildschirms bei Inaktivität nach Zeit
☐	Die Rechner sind durch Anti-Viren-Software geschützt (Programm-, Geräte- und Webkontrolle)

1.3.	**Zugriffskontrolle**
Damit sind Maßnahmen gemeint, die gewährleisten, dass die zur Benutzung der Datenverarbeitungs-verfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	
Unsere Maßnahmen zum Schutz gegen Zugriff auf personenbezogene Daten durch Unbefugte:	
☐	Verwendung von benutzerbezogenen und individualisierten Anmeldeinformationen
☐	Die Passworte haben eine Mindestkomplexität (Sonderzeichen, Anzahl der Zeichen)

☐	Es bestehen auf Applikations- und Datenebene differenzierte Berechtigungsstufen
☐	Für eventuelle (Fern-)Wartungsmaßnahmen sind Sicherheitsregeln in Kraft
☐	Es erfolgt eine Verschlüsselung der auf den Arbeitsrechnern gespeicherten Passwort-Daten, sowie sämtlicher Daten, die auf mobilen Backup-Medien (z.B. externe Laufwerke) gespeichert sind
☐	Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken
☐	Verbot des Einsatzes privater Datenträger (beispielsweise USB-Sticks)

1.4.	**Verschlüsselung**
Die Verschlüsselung von personenbezogenen Daten, sowie Passworten, die den Zugriff zu personenbezogenen Daten ermöglichen ist eine Möglichkeit diese gegen die Kenntnisnahme durch Unbefugte zu schützen. Unter Verschlüsselung ist ein Verfahren zu verstehen, durch das eine klar lesbare Information in eine nicht lesbare bzw. interpretierbare Zeichenabfolge umgewandelt wird.	
Unsere Maßnahmen in Zusammenhang mit der Verschlüsselung von Daten:	
☐	Auswahl eines geeigneten kryptographischen Verfahrens (z.B. VeraCrypt) erfolgt unter Berücksichtigung des aktuellen Stands der Technik
☐	Insbesondere verschlüsselt werden leicht mobil zu entfernende personenbezogene Daten (z.B.: auf externen Laufwerken) sowie sämtliche abgespeicherte Passworte.
☐	Regelmäßige Prüfung der Verschlüsselungsverfahren (insb. auf Sicherheitslücken) und Anpassung dieser an die aktuellen technischen Entwicklungen (insb. Aktualisierung der eingesetzten Software)

1.5.	**Trennungskontrolle**
Damit sind Maßnahmen gemeint, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	
Unsere Maßnahmen zur Trennungskontrolle:	
☐	Logische bzw. technische Trennung von Daten
☐	Benutzerprofile / Trennung von Mandantenakten
☐	Definierung von Zugriffsberechtigungen
☐	Speicherung in unterschiedlichen Speicherbereichen (Einzelrechner, interner Server, extern)

2	Integrität

Die Sicherstellung der Integrität bezieht sich insbesondere auf Eingabe und Weitergabe von personenbezogenen Daten sowie alle Maßnahmen, die generell zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung und zur Gewährleistung der Aktualität der Daten beitragen.

Maßnahmen zur Sicherstellung der Integrität:

☐	Einsatz von Verschlüsselungstechniken (SSL) im Bereich Internet- und E-Mail-Verkehr
☐	Spezifische Zuweisung von Berechtigungen hinsichtlich: Physische Akten, Rechner, interner Server, externe Datensysteme, bzw. -sammlungen
☐	Prozesse zur Aufrechterhaltung der Aktualität von Daten
☐	Dokumentierung des Hard- und Softwarebestandes und Führung eines Bestandsverzeichnisses
☐	Anonymisierung von personenbezogenen Daten (siehe Ziffer 2.1.)
☐	Weitergabekontrolle (siehe Ziffer 2.2.)
☐	Eingabekontrollen (siehe Ziffer 2.3.)

2.1.	Anonymisierung

Anonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Unsere Maßnahmen in Zusammenhang mit der Anonymisierung personenbezogener Daten:

☐	Anonymisierungsgebot ist Bestandteil im Rahmen des Datenschutzkonzepts des Unternehmens. Insbesondere erfolgen gemeinsame Fallbesprechungen der Berater*innen zur Qualitätssicherung grundsätzlich mit anonymisierten Daten.
☐	Anonymisierung von Daten entsprechend unterschiedlicher Schutzbedarfskategorien von Daten.

2.2.	Weitergabekontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Unsere Maßnahmen zum Schutz bei Datenübertragungen:

☐ Verschlüsselung von Daten und Datenträgern in Abhängigkeit von deren Schutzbedürftigkeit und Risikopotenzial (mobile Datenspeicher) insbesondere mittels Datei- und Festplattenverschlüsselung auf Hard- oder Softwarebasis (z.B. VeraCrypt)
☐ Verschlüsselung der Übertragung von Daten (SSL) bei der Übertragung über öffentliche Netze
☐ Ggfls. Sorgfältige Auswahl von Transportdienstleistern

2.3.	**Eingabe- und Verarbeitungskontrolle**
Damit sind Maßnahmen gemeint, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-Systemen bzw. -Anwendungen eingegeben, verändert oder entfernt worden sind.	
Unsere Maßnahmen zur Überprüfung von Eingaben, Änderungen und Löschungen:	
☐ Festlegung der Befugnisse für die Eingabe und der Bearbeitung von Daten	
☐ Aufzeichnung / Protokollierung von entsprechenden, an Systemen durchgeführten Aktionen (Logfiles)	
☐ Einsatz von Protokollierungs- und Protokollauswertungssysteme durch externe Dienstleister	

3.	**Sicherstellung und Wiederherstellung der Verfügbarkeit**
Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Verfügbarkeit auf Dauer gewährleisten.	
Unsere Maßnahmen zur Sicherstellung der Verfügbarkeit auf Dauer:	
☐ Beschaffung von geprüfter Hardware	
☐ Einsatz geprüfter Standardsoftware aus sicheren Quellen	
☐ Regelmäßige Durchführung von Datensicherungen	
☐ Getrennte Aufbewahrung von Datenbeständen, die zu unterschiedlichen Zwecken erhoben wurden oder die zu unterschiedlichen Schutzbedarfskategorien gehören	
☐ Büro-Inhaltsversicherung zur Finanzierung der Wiederherstellung im Zerstörungsfall	
☐ Betreuung der IT durch qualifizierten Dienstleister	
☐ Regelmäßiges Testen der Datenwiederherstellung	

4	Überprüfung und Evaluierung der Datensicherheit

Maßnahmen um die getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit laufend aktuell zu halten und kritisch zu begutachten. Diese Pflicht erstreckt sich auf alle technischen und organisatorischen Maßnahmen (Ziff. 1 bis 3).

Unsere Maßnahmen zur regelmäßigen Überprüfung und Evaluierung:

- ☐ Es ist ein Datenschutzkonzept vorhanden welches mindestens einmal jährlich überprüft wird
- ☐ Das Datenschutzkonzept wird an sich ändernde Bedingungen angepasst
- ☐ Es gibt ein Konzept zum Umgang mit bzw. Melden von Datenpannen
- ☐ Alle Beschäftigten bzw. Berater*innen werden regelmäßig – mindestens einmal jährlich geschult
- ☐ Wenigstens einmal jährlich findet eine Konsultation mit einem externen IT-Spezialisten statt

5	Auftragskontrolle

Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten, die in unserem Auftrag von Dritten verarbeitet werden, entsprechend den datenschutzrechtlichen Bestimmungen behandelt werden.

Unsere Maßnahmen zur Auftragskontrolle:

- ☐ Es sind Kriterien zur Auswahl der Auftragnehmer festgelegt (Referenzen, Zertifizierungen)
- ☐ Es gibt detaillierte schriftliche Regelungen der Auftragsverhältnisse
- ☐ Auftragnehmer haben mindestens eine/n Datenschutzbeauftragte/n bestellt
- ☐ Soweit für die vereinbarte Auftragsverarbeitung externe Server und/oder Cloud-Lösungen eingesetzt werden müssen sich die genutzten Rechenzentren in der EU befinden und die Standorte bzw. Länder hinsichtlich Datensicherheit nicht als kritisch eingestuft sein. Die Datenkommunikation mit Auftragsdienstleistern hat auf jeden Fall verschlüsselt zu erfolgen.