Beschreibung Technische und organisatorische Maßnahmen (TOMs)

der Organisation:

SaSG GmbH & Co. KG

Hinweis
Allgemeines Gleichbehandlungsgesetz (AGG) Aus Gründen der leichteren Lesbarkeit wird in diesem Dokument auf eine geschlechterspezifische Differenzierung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für alle Geschlechter.

Anlage 2 - Datensicherheit Beschreibung TOMs

Technische und organisatorische Maßnahmen i. S. d. Art. 32 Abs. 1 DSGVO

Inhalt

Anlage 2 - Datensicherheit Beschreibung TOMs

Technische und organisatorische Maßnahmen i. S. d. Art. 32 Abs. 1 DSGVO

1 Einleitung

Datensicherheit ist ein wichtiger integrierter Part im Datenschutz. Über Datensicherheit werden die technischen und organisatorischen Maßnahmen geregelt, die erforderlich sind, um den Schutz von personenbezogenen Daten bei automatisierter Verarbeitung, also in Systemen oder Programmen, zu gewährleisten.

Im Fall des Einbezugs von Auftragsverarbeitern müssen diese ebenfalls auf die Einhaltung von Datensicherheit geprüft werden (Art. 28 DSGVO).

Die Europäische Datenschutzgrundverordnung (DSGVO) enthält in Art. 32 Abs. 1 DSGVO Vorgaben darüber, dass personenbezogene Daten über adäquate technische und organisatorische Maßnahmen sicher verarbeitet werden müssen. Die Umsetzung der Schutzziele (= Maßnahmen) bleibt dabei dem Verantwortlichen*, „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen*" (Art. 32 DSGVO) selbst überlassen.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Für eine automatisierte Verarbeitung (also vor allem per Hard- und Software) nennt die DSGVO verschiedene Kontrollbereiche, die jeweils verschiedene Unterpunkte beinhalten:

(1) Pseudonymisierung und Verschlüsselung wo immer möglich
(2) Vertraulichkeit
(3) Integrität
(4) Verfügbarkeit und Belastbarkeit
(5) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Für nicht-automatisierte Verarbeitungen von personenbezogenen Daten sind die oben genannten Kontrollbereiche nach dem Gesetzeswortlaut nicht direkt anwendbar. Es wird jedoch empfohlen, für einen bestmöglichen Schutz auch in diesen Fällen die Datensicherheit in Anlehnung an die Kontrollbereiche zu organisieren.

2 Organisatorisches

Die gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus und gibt den Mitarbeitern schriftliche Vorgaben in Form von Arbeitsanweisungen, Richtlinien und Merkblätter für die Einhaltung. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO verpflichtet.

Einige diesen Bereich betreffende Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie entweder in die Verantwortung von Auftragsverarbeitern fallen und daher gesondert geregelt und geprüft werden oder da aus Gründen der Vertraulichkeit nicht alle Details veröffentlicht werden sollen.

3 Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der betrieben werden.

3.1 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Wo immer möglich, werden personenbezogene Daten ausschließlich pseudonymisiert (also ohne direkte Erkennbarkeit einer betroffenen Person) verarbeitet. Zudem sollten Daten, wo immer möglich, ausschließlich verschlüsselt versendet oder gespeichert werden. Dabei gilt das Prinzip der Verhältnismäßigkeit.

3.2 Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

3.2.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

Maßnahmen	Bemerkung
Am Standort gibt es maschinelle Zutrittskontrollsysteme zur Überwachung des Betretens und Verlassens eines Gebäudes.	
Es handelt sich um freistehenden Gebäudekomplex	
Die Verteilerräume oder -bereiche der Gebäudetechnik sind gegen unbefugten Zutritt gesichert.	
Es ist eine durchgängige Außenhautsicherung mit einbruchshemmenden Maßnahmen vorhanden.	
Es gibt Sicherungsmaßnahmen gegen Überfälle.	
Die Unternehmensserver werden in einem abgeschlossenen und zutrittsgesicherten Raum betrieben.	

3.2.2 Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Maßnahmen	Bemerkung
Es ist sichergestellt, dass Benutzer nur Zugang zu den Netzdiensten bekommen, zu deren Nutzung sie ausdrücklich befugt sind.	
Es ist sichergestellt, dass nur berechtigte Personen logischen Zugang zu den Netzwerkkomponenten haben.	
Es gibt ein formales Freigabeverfahren, welche Systeme und Applikationen mit personenbezogenen Daten zu durchlaufen haben, bevor diese Netzwerkzugang bekommen dürfen.	
Es ist sichergestellt, dass nur autorisierte Geräte von privaten Personen oder Besuchern logischen Zugang zum Netzwerk der Organisation bekommen.	
Das WLAN ist vor unbefugtem Zugang gesichert.	

Softwareänderungen bei Wartungseinsätzen werden kontrolliert.	

3.2.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen	Bemerkung
Die Benutzer stellen sicher, dass ihre DV-Ausstattung, falls unbeaufsichtigt, ausreichend geschützt ist.	
Den Benutzern wird der Zeitpunkt der letztmaligen Verfahrensnutzung angezeigt.	
Die Entsorgung oder Weiterverwendung von Geräten, die mit Speichermedien ausgerüstet sind, ist geregelt.	

3.2.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen	Bemerkung
Personenbezogene Daten auf den Systemen werden physisch voneinander getrennt (Verarbeitung unterschiedlicher Datensätze auf getrennten Systemen).	
Personenbezogene Daten auf den Systemen werden logisch voneinander getrennt (unterschiedliche Datensätze in einer einheitlichen Datenbank werden je nach Zweck markiert (softwareseitige Unterscheidbarkeit)).	
Die im Unternehmen eingesetzten Systeme sind mandantenfähig.	
Die Mandantenfähigkeit für die davon betroffenen Verfahren ist durchgängig realisiert.	

3.3 Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

3.3.1 Weitergabekontrolle

Maßnahmen, 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen	Bemerkung
Alle Personen, die mit der Verarbeitung/Nutzung personenbezogener Daten beschäftigt sind, sind zur Einhaltung der Vertraulichkeit verpflichtet.	

Allen neuen Mitarbeitern werden bei der Verpflichtung zur Vertraulichkeit Informationen zum Datenschutz ausgehändigt.	
Die Mitarbeiter, die personenbezogene Daten verarbeiten/nutzen, werden durch Datenschutzschulungen auf datenschutzgerechtes Verhalten am Arbeitsplatz geschult worden.	
Angemessene Sicherheitsmaßnahmen für den physischen Transport von Datenträgern (inkl. Papier) sind umgesetzt.	
Es ist sichergestellt, dass Daten nur an die vom Auftraggeber festgelegten oder der Zweckbestimmung nach richtigen Adressaten übermittelt werden.	

3.3.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen	Bemerkung
Es ist geregelt, wie lange diese protokollierten Daten aufbewahrt werden dürfen.	
Diese Daten unterliegen einer strengen Zweckbestimmung.	
Die protokollierten Daten sind gegen unbefugte Einsicht oder Manipulation geschützt.	

3.4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) und c) DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Maßnahmen	Bemerkung
Die Risikofaktoren gegen die Aufrechterhaltung des DV-Betriebes wurden untersucht.	
Die Systeme sind gegen Ausfall abgesichert.	
In regelmäßigen Abständen wird überprüft, ob die Versorgung mit Fernmelde- und Datenleitungen, Strom, Wärme und Wasser noch ausreichend ist.	
Die Versorgungsleitungen verlaufen unterirdisch.	
In den Rechnerräumen befinden sich keine wasserführenden Leitungen.	
Es werden ausreichend dimensionierte USVs eingesetzt.	
Die USV ist auf eine Versorgungszeit für 20 Minuten ausgelegt.	

Die USV-Anlage verfügt über Überspannungsschutzeinrichtungen.	
Es gibt Blitzschutzeinrichtungen.	
Im Serverbereich befinden sich keine brennbaren Gegenstände.	
Ein Frühwarnsystem mit automatischen Brandmeldern ist installiert.	
Es sind ausreichend geeignete Feuerlöscher sowie das richtige Löschmittel im Einsatz und dabei wird auf Einheitlichkeit geachtet.	
Es gibt Backup-Rechenzentren/Ausweichrechner/Ausweichräume).	
Es existiert ein Notfallkonzept für das Netzwerk.	
Es werden regelmäßige Backups durchgeführt.	
Die Datenträger, wo die Backups gespeichert sind, sind verschlüsselt	
Die Backups sind vor Diebstahl und Zerstörung geschützt.	
Die Backups werden jährlich getestet, ob Sie brauchbar sind.	
Es gibt eine Notabschaltung der Stromversorgung.	
Es gibt ein Ausweichrechenzentrum.	
Antivirensoftware wird eingesetzt.	

3.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d) DSGVO)

3.5.1 Organisatorische Sicherheitskriterien

Organisatorische Sicherheit beschreibt alle organisatorische Maßnahmen (Handlungsanweisungen, Vorgehensweisen, etc.) zur Gewährleistung und Verbesserung der Sicherheit.

Maßnahmen	Bemerkung
Eine regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte werden durchgeführt.	
Ein Datenschutz-Managementsystem (DSMS) ist eingeführt.	