

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

(TOMs)

Nachfolgend handelt es sich um eine Aufstellung der Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten gem. Art. 32 Abs. 1 der DSGVO, die von dogado GmbH (im Folgenden: Auftragnehmer) im Auftrag ihres Kunden (im Folgenden: Auftraggeber) verarbeitet werden.

Die dogado GmbH stellt dem Auftraggeber die erforderliche Hard- und Software zur Datenverarbeitung entsprechend dem jeweiligen Auftrag zur Verfügung. Allein der Auftraggeber entscheidet darüber, welche personenbezogenen Daten und in welcher Weise über bereitgestellten Datenverarbeitungsanlagen verarbeitet werden. Die dogado GmbH sorgt für die technische Einsatzbereitschaft der Systeme entsprechend den vertraglichen Vereinbarungen und protokolliert, welche Anlagen durch den Auftraggeber in welchem Umfang genutzt werden. Die dogado GmbH hat keinerlei Einfluss auf die durch den Auftraggeber durchgeführten Datenverarbeitungsvorgänge auf den bereitgestellten Systemen.

Die dogado GmbH verfügt über weitreichende Sicherheitskonzepte und Prozesse angelehnt an ISO 27001 – Standards zu den einzelnen Bestandteilen der „Technischen und organisatorischen Maßnahmen“.

1. VERTRAULICHKEIT (Art. 32 Abs. 1 lit. b DSGVO)

1.1. Zutrittskontrolle

Maßnahmen zur Zutrittskontrolle entsprechend eines Schutzzonenkonzepts sollen den unbefugten Zutritt zu Datenverarbeitungsanlagen (insbesondere in Rechenzentren und nicht öffentlichen Bereichen) verhindern:

- Zutrittskontrollsystem: Ein Schließsystem in Form einer Authentifizierung mittels zumindest eines Faktors (z.B. Transponder, Chipkarte, Klingelsystem mit Personenkontrolle per Bild und Ton) ermöglicht den Zutritt zu Datenverarbeitungsanlagen erst nach positiver Zutrittsprüfung.
- Schlüsselregelung: Schlüsselausgaben an Personen zum Zutritt zu Datenverarbeitungsanlagen werden dokumentiert.
- Protokollierung der Besucher: Besucher, die Zutritt zu nicht öffentlichen Bereichen erhalten (z.B. im Falle von Hardware- Austausch durch den Hersteller) werden in einem Besucherbuch erfasst.
- Besucher oder sonstige Dritte sind gemäß den Vorgaben in Zonen mit erhöhter Sicherheitsanforderung zu begleiten.
- Eingeschränkter Zutritt über elektronische Türsicherung mit Protokollierung: Der Zutritt zu nicht öffentlichen Bereichen ist durch Öffnungsmeldung (allenfalls Einbruchsmeldeanlagen oder Überwachung von Zugangskartenverwendung) abgesichert.
- Videoüberwachung: Datenverarbeitungsanlagen werden per Videoüberwachung durch eingesetzte und datenschutzrechtlich verpflichtete Unterauftragnehmer gesichert.

1.2. Zugangskontrolle

Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung vermeiden unbefugten Zugang zu Datenverarbeitungssystemen.

- Passwortvergabe: Ein Zugang zu den Datenverarbeitungssystemen ist grundsätzlich nur mittels einer Kombination aus einem Benutzernamen und dem zugeordneten Passwort möglich. Sofern technisch möglich, ist eine angemessene Multi-Faktor- oder kontinuierliche Authentifizierungen implementiert.
- Passworrichtlinie: Passwörter für Datenverarbeitungsanlagen haben Mindest-Komplexitätsanforderungen der unternehmensweiten Richtlinie zu entsprechen. Einhaltung dieser Komplexitätsanforderungen werden automatisch geprüft und nicht adäquate Passwörter abgelehnt. Passwörter müssen durch Mitarbeiter regelmäßig geändert werden.

- Administrativer Zugriff: Sämtliche Datenverarbeitungssysteme sind zu Wartungszwecken ausschließlich über freigegebene IP-Adressbereiche und verschlüsselt erreichbar (z.B. VPN- Beschränkungen).
- Firewall: Die Infrastruktur ist durch den Einsatz von kontinuierlich gewarteten Firewalls, sowohl in Software- als auch in Hardware-Form, geschützt. Diese dienen dazu, eine starke Verteidigungslinie gegen externe Bedrohungen wie Hackerangriffe, Viren und verschiedene Formen von Malware zu schaffen.
- Endgerätesicherheit: Systeme, die für den Zugriff auf Datenverarbeitungssysteme verwendet werden, sind mit einer zentral administrierten Endpoint-Protection-Lösung versehen und werden kontinuierlich aktualisiert. Zudem werden Systeme, die Kundenservices bereitstellen, gemäß den im Hauptvertrag festgelegten Vereinbarungen, wie zum Beispiel mit Anti-Viren-Software (Signaturscanner) ausgestattet.
- Die Systeme unterliegen gemäß den Vereinbarungen im Hauptvertrag einem kontinuierlichen Patch- und Update-Management.
- Verschlüsselung von mobilen Datenträgern: Bei der Verwendung mobiler Datenträger oder Geräte werden diese und/oder deren Inhalte stets nach dem aktuellen Stand der Technik verschlüsselt, um die Datensicherheit zu gewährleisten.

1.3. Zugriffskontrolle

Darunter fallen Maßnahmen, die unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems hintanhalten sollen.

- Zuordnung von Benutzerrechten: Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.
- Sichere Aufbewahrung von Datenträgern: Datenträger, die personenbezogene Daten enthalten, werden verschlossen oder verschlüsselt gelagert.
- Verwaltung der Rechte durch einen eingeschränkten Personenkreis: Ausschließlich berechnete Systemadministratoren sind in der Lage, Rechte anderer Personen zu Datenverarbeitungssystem zu verwalten. Der Kreis der berechtigten Systemadministratoren wird auf die kleinstmögliche Auswahl von Personen reduziert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.
- Protokollierung der Zugriffe: Zugriffe auf Dienste (z. B. Webdienste) werden in Log-Files protokolliert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat jedoch keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.
- Ordnungsgemäße Vernichtung von Datenträgern: Datenträger, die personenbezogene Daten enthalten werden gemäß DIN 66399 vernichtet.

1.4. Trennungskontrolle

Unter Trennungskontrolle werden Maßnahmen verstanden, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten, getrennt verarbeitet werden.

- Festlegung von Datenbankrechten: Der Zugriff von Systemen und Benutzern auf Datenbanken wird auf die jeweils notwendigen Daten eingeschränkt. Das Need-To-Know-Prinzip findet Anwendung.
- Trennung von Produktiv- und Testsystemen: Produktiv- und Testumgebungen werden isoliert voneinander betrieben. Ein Zugriff einer Umgebung auf Daten der jeweils anderen Umgebung wird durch den Einsatz von z.B. getrennten Datenbanksystemen und Serversystemen unterbunden.
- Logische Mandantentrennung: Durch den Einsatz softwareseitiger Mechanismen wird eine Trennung der Daten von Mandanten gewährleistet.
- Sofern rechtlich möglich und technisch sinnvoll, werden personenbezogene Daten pseudonymisiert, sodass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.

2. INTEGRITÄT (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Das Ziel der Weitergabekontrolle besteht darin, effektive Kontrollmechanismen zu implementieren, um die sichere Weitergabe datenschutzrelevanter Informationen sowohl innerhalb der Organisation als auch an externe Partner zu gewährleisten. Dabei werden Daten vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen auf dem Transportweg (manuell oder elektronisch) z. B. während der Übertragung, Übermittlung oder Speicherung auf Datenträger sowie bei der nachträglichen Überprüfung, geschützt. Die Weitergabe von Informationen erfolgt mittels sicherer Übertragungstechniken, die adäquate Verschlüsselung und Schutzmechanismen beinhalten. Bei der Übermittlung sensibler Daten über öffentliche Netzwerke ist zudem die Verwendung von Ende-zu-Ende-Verschlüsselung erforderlich.

- Verschlüsselung/Tunnelverbindung (VPN = Virtual Private Network):
- Verschlüsselung auf dem Transportweg (insbesondere https/SSL)
- Protokollierung/Auswertung
- Richtlinie zur Informationsklassifizierung

2.2. Eingabekontrolle

Unter Eingabekontrolle verstehen sich Maßnahmen, die nachträglich feststellen lassen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Die Eingabekontrolle der Daten kann ausschließlich durch den Kunden umgesetzt werden, weil der Auftragnehmer keinen darauf Einfluss hat, wie der Auftraggeber die zur Verfügung gestellten Systeme verwendet. Auf Seiten des Auftragnehmers werden folgende technischen Vorkehrungen dafür implementiert:

- Rollen- und Benutzerrechte: Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender abgestufter Benutzerrechte eingeschränkt.
- Protokollierungs- und Protokollauswertungssysteme (Logserver)
- Protokollierung von Dateneingaben: Bei Änderungen durch den Auftragnehmer werden die Administrationszugriffe adäquat protokolliert.

3. VERFÜGBARKEIT UND BELASTBARKEIT (Art. 32 Abs. 1 lit. b DSGVO)

Hierunter fallen Maßnahmen zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust von Daten:

- Unterbrechungsfreie Stromversorgung in Serverräumen (Rechenzentren)
- Um eine erhöhte Verfügbarkeit zu gewährleisten, sind die Serverräume durch unterbrechungsfreie Stromversorgungen (USV) geschützt. Dieser Schutz ist in zwei Stufen konzipiert. Im Falle eines Stromausfalls aktiviert sich automatisch ein Notstromaggregat, welches die Stromversorgung der Serverräume sicherstellt.
- Klimaanlage in Serverräumen (Rechenzentren)
- Eine für den Betrieb von Serversystemen angemessene Temperatur und Luftfeuchtigkeit wird in Serverräumen durch ausreichend dimensionierte Klimaanlage gewährleistet.
- Feuer- und Rauchmeldeanlagen in Serverräumen (Rechenzentren)
- Durch den Einsatz von Feuer- und Rauchmeldeanlagen wird ein Brand frühzeitig erkannt. Feuerlöschanlagen löschen auftretende Brände.
- Datensicherungskonzept und Aufbewahrung von Datensicherungen
- Datensicherungen von personenbezogenen Daten werden nur nach Vereinbarung bzw. gemäß des abgeschlossenen Hauptvertrages angefertigt und auf separaten und für Datensicherungen dediziert eingesetzten Systemen aufbewahrt.
- Systemkritische Instanzen werden durch Monitoring überwacht. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

Datenschutz-Management: Der Auftragnehmer hat ein Datenschutzmanagementsystem (DSMS) etabliert, das den Schutz der personenbezogenen Daten sicherstellt. Dieses hat das Ziel die an den Datenschutz gestellten Anforderungen, z.B. die Eintrittswahrscheinlichkeit für Datenpannen oder Datenschutzverstöße zu verringern und im Falle eines Eintritts den Schaden und das Risiko für die betroffenen Personen zu begrenzen, sicherzustellen.

4.2. Incident-Response-Management

Der Auftragnehmer verfügt über einen Incident-Management-Prozess nach ISO27001-Standard, der darauf abzielt, Sicherheitsvorfälle schnell zu identifizieren, zu analysieren und nachhaltig zu beheben, um Auswirkungen auf die Geschäftstätigkeit zu minimieren und die Wiederherstellung der normalen Betriebsabläufe zu beschleunigen. Dieser berücksichtigt die Anforderungen der DSGVO und geltende rechtliche Vorgaben zur Netz- und Informationssystemsicherheit (insbesondere NIS-Richtlinien).

4.3. Datenschutzrechtliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Der Auftragnehmer stellt innerhalb seiner Möglichkeiten sicher, dass durch Voreinstellung nur Daten, die für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind, verarbeitet werden. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

4.4. Auftragskontrolle

Der Auftragnehmer stellt einen einfachen Auftragsverarbeitungsvertrag iSd Art. 28 DSGVO bereit. Der Auftraggeber ist verpflichtet nach seinen Ansprüchen an die Schutzbedürftigkeit seiner zu verarbeitenden Datenkategorien allenfalls auf darüberhinausgehende angemessene Garantien hinzuwirken. Grundsätzlich hat der Auftragnehmer weder Kenntnis noch Einfluss darauf, ob personenbezogene oder sonstige sensible Daten auf den bereitgestellten Systemen gespeichert oder verarbeitet werden. Sofern der Auftragnehmer jedoch beispielsweise im Rahmen von Supportleistungen oder Wartungen Zugriff auf bestimmte Kundenumgebungen erhält, wird dies protokolliert.

Bei der Auswahl von Unterauftragnehmern, die personenbezogene Daten im Rahmen des Auftrags verarbeiten, werden nur solche Auftragnehmer ausgewählt, die mindestens die gesetzlich vorgeschriebenen Anforderungen an die Verarbeitung von personenbezogenen Daten einhalten und entsprechend gemäß Art. 28 DSGVO verpflichtet. Im Rahmen einer nachhaltigen Corporate Compliance wird auf die Einhaltung weiterer rechtlichen Vorgaben zur Auswahl von Vertragspartnern geachtet. Während laufender Beauftragung werden Unterauftragnehmer regelmäßig auf die Einhaltung der zugesicherten technischen und organisatorischen Maßnahmen bei der Verarbeitung von personenbezogenen Daten überprüft.