TOMs: Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

Als Organisation, die selbst oder im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen Sie geeignete technische und organisatorische Maßnahmen treffen, um die Vorschriften der Datenschutzgesetze zu erfüllen.

Wichtige Grundsätze der DSGVO gelten dabei als der Leitfaden, der Sie bei der Erarbeitung der Maßnahmen lenken wird, so zum Beispiel die Datenminimierung durch
→ **Privacy by Design / Privacy by Default:** Das heißt, Sie sollten so wenige Daten wie möglich bzw. nur so viele Daten wie unbedingt nötig sammeln oder verarbeiten und diese Daten auch nur so kurz wie nötig speichern. Bereits bei der Erhebung von Daten wählen Sie daher die Voreinstellungen so aus, dass diese Grundsätze berücksichtigt werden (Opt-in).

Die DSGVO sieht eine Dokumentationspflicht der getroffenen Maßnahmen vor. Es ist allerdings auch klar geregelt, dass sämtliche Maßnahmen unter Berücksichtigung von:
→ **Stand der Technik**
→ **Aufwand**
→ **Risiko** erfolgen muss.
Das heißt, Sie müssen nachweisen, dass Sie mit personenbezogenen Daten sorgsam umgehen, wie dieser Umgang im Einzelnen aussieht, ist je nach Organisation (Art, MitarbeiterInnenanzahl, Art der verarbeiteten Daten,...) jedoch verschieden. Die Zumutbarkeit des Aufwandes sowie das durch die Datenverarbeitung entstehende Risiko sind dabei wichtige Parameter.

Rund um die Verarbeitung personenbezogener Daten herrscht →**Dokumentationspflicht**. Diese kann ähnlich wie die Buchhaltung eines Unternehmens gesehen werden: Es handelt sich um einen laufenden Prozess, der kontinuierlicher Evaluierung und ggf. Anpassungen bedarf. Im Anlassfall können Sie dann sämtliche Maßnahmen, Ereignisse, Entscheidungen, etc., vorlegen.

Wir möchten Ihnen mit diesem Dokument einen Leitfaden in die Hand geben, um bereits bestehende Maßnahmen zu identifizieren, ggf. nachzubessern und zu dokumentieren.

Organisation: .....

Verantwortliche/r: .....

Straße .....

PLZ, Ort .....

Walter Wratschko | Geprüfter Datenschutz-Experte
Schwerpunkt Alpe Adria Region
Khevenhüllerstraße 30/1 | 9020 Klagenfurt
Telefon +4369915043860 | Mobil +4369915043860
Mail der@dsgvo-scout.at | web dsgvo-scout.at

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.1. Zutrittskontrolle:

Dokumentieren Sie, mit welchen Mitteln in Ihrem Betrieb oder Verein gewährleistet wird, dass unbefugte Personen keinen Zugriff auf Daten haben. Dazu gehört auch die Zugangskontrolle in Ihre Büro- oder Vereinsräumlichkeiten: Wer besitzt z.B. einen Schlüssel? Beschreiben Sie, wie Sie dafür Sorge tragen, dass sowohl Daten in Papierform nicht für Unbefugte zugänglich sind (z.B. versperrbare Aktenschränke), als auch unbefugter Zugriff auf die IT verhindert wird (passwortgeschützte Computer, Systeme,...)
Andere Maßnahmen können unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen sein. Server,Telekommunikations-anlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Organisatorische Maßnahmen können z.B. Dienstanweisungen sein: Verschließen der Diensträume bei Abwesenheit, Sperren des Computers, wenn der Arbeitsplatz verlassen wird, usw.

Technische Maßnahmen:

- ○ Alarmanlage
- ○ Automatisches Zugangskontrollsystem
- ○ Biometrische Zugangssperren
- ○ Chipkarten / Transpondersysteme
- ○ Manuelles Schließsystem
- ○ Sicherheitsschlösser
- ○ Schließsystem mit Codesperre
- ○ Absicherung der Gebäudeschächte
- ○ Türen mit Knauf Außenseite
- ○ Klingelanlage mit Kamera
- ○ Videoüberwachtung der Eingänge

Organisatorische Maßnahmen:

- ○ Schlüsselregelung / Liste
- ○ Empfang / Rezeption / Pförtner
- ○ Besucherbuch / Protokoll der Besucher
- ○ Mitarbeiterlinnen / Besucher/innen-Ausweise
- ○ Besucherlinnen in Begleitung der Mitarbeiter/innen
- ○ Sorgfalt bei Auswahl des Wach, - Reinigungspersonals

Weitere Maßnahmen bitte hier beschreiben:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.2. Zugangskontrolle:

Beschreiben Sie hier Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können: Mit Zugangskontrolle ist das Verhindern der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen:

- ○ Login mit Benutzername + Passwort
- ○ Login mit biometrischen Daten
- ○ Anti-Viren-Software Server
- ○ Anti-Viren-Software Client
- ○ Anti-Viren-Software Mobile Geräte
- ○ Firewall
- ○ Intrusion Detection Systeme
- ○ Mobile Device Management
- ○ VPN bei Remotezugriffen
- ○ Verschlüsselung von (externen) Datenträgern
- ○ Verschlüsselung von Smartphones
- ○ Gehäuseverriegelung
- ○ BIOS-Schutz durch separates Passwort
- ○ Sperre externer Schnittstellen (USB)
- ○ Automatische Desktopsperre
- ○ Verschlüsselung von Notebooks / Tablets

Organisatorische Maßnahmen:

- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Zentrale Passwortvergabe
- Richtlinie “Sicheres Passwort”
- Richtlinie “Löschen / Vernichten”
- Richtlinie “Clean Desk”
- Allgemeine Richtlinie Datenschutz und / oder Sicherheit
- Anleitung Manuelle Desktopsperre

Weitere Maßnahmen bitte hier beschreiben:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.3. Zugriffskontrolle:

Dokumentieren Sie hier alle Maßnahmen, die Sie setzen um Folgendes zu gewährleisten:

Berechtigte zur Nutzung eines Datenverarbeitungssystems können ausschließlich auf Daten, die für sie freigeschalten sind, zugreifen; Personenbezogene Daten können bei der Benutzung und Verarbeitung sowie nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Dies können Sie unter anderem durch Berechtigungskonzepte umsetzen, wobei sowohl der Inhalt als auch die möglichen Zugriffsfunktionen je nach Benutzergruppe unterschiedlich sein können (Beispiel: MitarbeiterInnen des Verkaufs haben keinen Zugriff auf Personaldaten im Unternehmen; nur ein eingeschränkter Personenkreis darf Kundendaten anlegen, ein weiterer Personenkreis diese z.B. nur ansehen)

Definieren Sie Verantwortlichkeiten zur Dokumentation von Vergabe und Entzug von Berechtigungen (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Kündigung,...)

Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der AdministratorInnen zu richten.

Technische Maßnahmen:

- ○ Aktenshredder (mind. Stufe 3, Cross Cut)
- ○ Externer Aktenvernichter (DIN 32757)
- ○ Physische Löschung von Datenträgern
- ○ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten

Organisatorische Maßnahmen:

- ○ Einsatz von Berechtigungskonzepten
- ○ Minimale Anzahl an Adrministratoren
- ○ Datenschutztresor
- ○ Verwaltung der Benutzerrechte durch Administratoren

Weitere Maßnahmen bitte hier beschreiben:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

1.4. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Pseudonymisierung bedeutet, dass personenbezogene Daten in einer Art gespeichert werden, dass eine Zuordnung zu einer bestimmten Personen nicht mehr erfolgen kann. Diese zusätzlichen Informationen müssen gesondert aufbewahrt werden und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.

Technische Maßnahmen:

- ○ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (möglichst verschlüsselt)

Organisatorische Maßnahmen:

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

Weitere Maßnahmen bitte hier beschreiben:

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

2.1. Weitergabekontrolle

Hier beschreiben Sie Maßnahmen, die Folgendes gewährleisten:

Bei der elektronischen Übertragung von Daten oder während des Transports oder der Speicherung auf Datenträgern können diese nicht unbefugt gelesen, kopiert, verändert oder entfernt werden; es kann überprüft und festgestellt werden, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Um diese Vertraulichkeit zu gewährleisten können Sie z.B. Verschlüsselungstechniken und ein Virtual Private Network (VPN) einsetzen.
Werden Datenträger physisch transportiert, soll dies in verschließbaren Behältern erfolgen. Eine weitere Maßnahme ist z.B. eine Regelung zur datenschutzgerechten Vernichtung von Datenträgern.

Technische Maßnahmen:

- ○ E-Mail-Verschlüsselung
- ○ Einsatz von VPN
- ○ Protokollierung der Zugriffe und Abrufe auf / von Daten
- ○ Sichere Transportbehälter
- ○ Bereitstellung verschlüsselter Verbindungen (wie sftp, https)
- ○ Nutzung von Signaturverfahren

Organisatorische Maßnahmen:

- ○ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- ○ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- ○ Weitergabe in anonymisierter oder pseudonymisierter Form
- ○ Sorgfalt bei der Auswahl von Transportfirmen
- ○ Persönliche Übergabe mit Protokoll

Weitere Maßnahmen bitte hier beschreiben:

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

2.2. Eingabekontrolle

Beschreiben Sie hier, wie Sie gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

Beachten Sie bei diesem Thema auch, welche Daten protokolliert werden, wer Zugriff auf diese Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen:

- ○ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- ○ Manuelle oder automatisierte Kontrolle der Protokolle
- ○ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ○ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- ○ Klare Zuständigkeiten für Löschungen

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 (nicht Benutzergruppen)

Weitere Maßnahmen bitte hier beschreiben:

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

3.1. Verfügbarkeitskontrolle

Listen Sie auf, was Sie unternehmen, um personenbezogene Daten gegen zufällige Zerstörung oder Verlust zu schützen.

Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen, etc.

Technische Maßnahmen:

- ○ Feuer- und Rauchmeldeanlagen
- ○ Feuerlöscher im Serverraum
- ○ Serverraumüberachung Temperatur und Feuchtigkeit
- ○ Klimatisierung des Serverraums
- ○ USV
- ○ Schutzsteckdosenleisten im Serverraum
- ○ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)
- ○ RAID System / Festplattenspiegelung
- ○ Videoüberwachung Serverraum
- ○ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum

Organisatorische Maßnahmen:

- ○ Backup & Recovery-Konzept (ausformuliert)
- ○ Kontrolle des Sicherungsvorgangs
- ○ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- ○ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- ○ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- ○ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
- ○ Getrennte Partitionen für Betriebssysteme und Daten

Weitere Maßnahmen bitte hier beschreiben:

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

4.1. Datenschutzmanagement

Technische Maßnahmen:

- ○ Verwendung von Software-Lösungen für Datenschutz-Management
- ○ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)
- ○ Sicherheitszertifizierung nach ISO 27001
- ○ Anderweitiges dokumentiertes Sicherheitskonzept
- ○ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt

Organisatorische Maßnahmen:

- ○ Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
- ○ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
- ○ Regelmäßige Sensibilisierung der Mitarbeiter, mindestes 1x jährlich
- ○ Interner / externer Informationssicherheits Beauftragter Name / Firma Kontakt
- ○ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- ○ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- ○ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Weitere Maßnahmen bitte hier beschreiben:

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

4.2. Incident - Response - Management

Listen Sie hier Maßnahmen auf, durch die im besten Fall Sicherheitsvorfälle frühzeitig erkannt und der Schaden begrenzt werden kann; beschreiben Sie weiters, welche Maßnahmen Sie gesetzt haben, um im Fall einer Sicherheitsverletzung den Schaden möglichst schnell und effizient zu beheben.

Technische Maßnahmen:

- ○ Einsatz einer Firewall, regelmäßige Updates
- ○ Einsatz eines Spamfilters, regelmäßige Updates
- ○ Einsatz eines Virenscanners, 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 Aufsichtsbehörde)
- ○ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- ○ Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
- ○ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
- ○ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Weitere Maßnahmen bitte hier beschreiben:

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

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

Listen Sie hier auf, wie Sie den Grundsatz der Privacy by Design / Privacy by Default umsetzen

Technische Maßnahmen:

- ○ Es werden nicht mehr personenbezogene Daten erhoben als unbedingt notwendig
- ○ Einfache Ausübung des Widerrufsrechts von Betroffenen durch technische Maßnahmen

Weitere Maßnahmen bitte hier beschreiben:

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

4.4. Auftragskontrolle (Outsourcing an Dritte)

Hierunter fallen Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung.
Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Organisatorische Maßnahmen:

- ○ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- ○ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- ○ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard Vertragsklauseln
- ○ Schriftliche Weisungen an den Auftragnehmer
- ○ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- ○ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen einer Bestellpflicht
- ○ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- ○ Regelung zum Einsatz weiterer Subunternehmer
- ○ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ○ Bei längerer Zusammenarbeit: LaufendeÜberprüfung des Auftragnehmers und seines Schutzniveaus
- ○ **Alternativ**: Hiermit versichern wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.

Weitere Maßnahmen bitte hier beschreiben:

Ausgefüllt am ..... für die Organisation durch:

Name .....

Funktion .....

Telefon .....

E-Mail .....

Vom Auftraggeber auszufüllen:

- ○ Es besteht noch Klärungsbedarf zu .....
- ○ TOM sind für den angestrebten Schutzzweck ausreichend
- ○ Vereinbarung Auftragsdatenverarbeitung kann geschlossen werden

Disclaimer:

Alle Informationen in diesem Workshop sind nach bestem Wissen und Gewissen zusammengestellt. Der Vortragende / Leiter dieses Workshops weist jedoch darauf hin, dass keine Haftung für die Richtigkeit, die Aktualität und die Vollständigkeit übernommen wird. Insbesondere ersetzt dieser Workshop keine rechtliche, organisatorische oder technische Beratung im Einzelfall.

Grundlage für die Erstellung der Unterlagen sind die von den TeilnehmerInnen mitgebrachten Aufzeichnungen und Unterlagen, deren Vollständigkeit und Plausabilität vom Vortragenden nicht überprüft werden können. Die TeilnehmerInnen sind sowohl für die Richtigkeit als auch die Vollständigkeit ihrer Unterlagen und Auskünfte verantwortlich, auch gegenüber den Nutzern der im Workshop erstellten Unterlagen. Die Erstellung gemäß der DSGVO erforderlichen Dokumente (beispielsweise Verfahrensverzeichnis, Löschkonzept, etc.) liegt in der alleinigen Verantwortung der TeilnehmerInnen.

Weiters schließt der Vortragende / Leiter des Workshops jegliche Haftung im Zusammenhang mit der möglichen Dateneinsicht, Datenverwendung und Datenweitergabe der TeilnehmerInnen untereinander aus.

Der Workshop behandelt die aktuelle Rechtslage der EU-Datenschutzgrundverordnung. Für mögliche Interpretationen und Auslegungsvarianten der Aufsichtsbehörden wird eine Haftung gleichermaßen ausgeschlossen wie für eine heute noch nicht absehbare Rechtssprechung. Andere gesetzliche Erfordernisse als die der EU-Datenschutzgrundverordnung werden nicht berücksichtigt.

Die Vertragspartner vereinbaren einen wechselseitigen Ausschluss der Haftung.

Quelle: a.s.k. Datenschutz, Sascha Kuhrau, https://www.bdsg-externer-datenschutzbeauftragter.de