Darstellung der technischen und organisatorischen Maßnahmen

Verantwortliche Stelle	Firma Sonnenschein GmbH, Sonnenscheinstraße 1, 12345 Sonnenschein am See, Geschäftsführerin Sabine Sonnenschein
Ansprechpartner	
Stand	

Dokumenthistorie

Datum	**Kurzbeschreibung/Grund für Änderung.**

1. Organisatorische Maßnahmen

☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?
☐ ja
Name:
☐ nein, dann bitte den Ansprechpartner für den Datenschutz angeben (Name, Kontaktdaten)

☐ Die Mitarbeiter wurden nachweislich über Datenschutz und Datensicherheit geschult bzw. informiert

☐ Alle Mitarbeiter sind nachweislich auf die Vertraulichkeit (Datengeheimnis), ggf. auf das Fernmeldegeheimnis und die Wahrung von Berufsgeheimnissen, verpflichtet

☐ Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z. B. technisch unterstützt oder durch Externe)

☐ Ein Datensicherheitskonzept/ Informationssicherheitsmanagement ist vorhanden

☐ Ein Datenschutzkonzept ist vorhanden

☐ Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am tt.mm.jjjj und Bestätigung s. Anlage x)

☐ Verhaltensregeln nach Art. 40 DS-GVO sind vorhanden (Unterwerfung am tt.mm.jjjj und Bestätigung s. Anlage x)

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☐ Sind schriftliche Zutrittsregelungen vorhanden?
- ☐ ja, im Dokument (z. B. im Datenschutzhandbuch):
- ☐ nein

☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
☐ Alarmanlage
☐ Automatisches Zutrittskontrollsystem, Ausweisleser
☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)
☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
☐ Sicherheitsschlösser
☐ Chipkarten-/Transponder-Schließsystem
☐ biometrische Kontrollsysteme (Fingerabdrücke o. ä.)
☐ Manuelles Schließsystem
☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)
☐ Magnetschleusen
☐ Werkschutz/Pförtner
☐ Empfang mit Anmeldung
☐ Sorgfältige Auswahl von Wachpersonal
☐ Sorgfältige Auswahl von Reinigungspersonal
☐ Lichtschranke/Bewegungsmelder
☐ Feuerfeste Türen
☐ Absicherung von Gebäudeschächten
☐ Fenstervergitterung
☐ Panzerglas
☐ Videoüberwachung der Zugänge

2.2 Zugangskontrolle

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

☐ Passwortvergabe
- ☐ Komplexität des Passworts
- ☐ Definierte Wechselfristen
- ☐ Anzahl der Fehleingaben beschränkt

☐ Chipkarte mit PIN/Passwort
☐ Authentifikation mit Benutzername/Passwort
☐ Biometrisches Merkmal mit PIN/Passwort
☐ Einsatz von VPN-Technologie
☐ Automatische Sperrung des Arbeitsplatzes

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.

- ☐ Schriftliches Berechtigungskonzepts vorhanden
- ☐ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
- ☐ Verwaltung der Rechte durch System-Administrator
- ☐ Anzahl der Administratoren auf das "Notwendigste" reduziert
- ☐ Gesicherte Nutzung von USB-Schnittstellen
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
  - ☐ Die Protokolle werden ausgewertet, zeitlicher Abstand: ….
- ☐ physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Einsatz von Akten-/Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399
- ☐ Verschlüsselung von Datenträgern
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ ordnungsgemäße Vernichtung von Datenträgern
- ☐ Löschungskonzept für Daten
- ☐ Protokollierung der Vernichtung

2.4 Trennungskontrolle

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

- ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Festlegung Technologie von Datenbankrechten
- ☐ Trennung von Daten verschiedener Auftraggeber

2.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass der Personenbezug von Daten nicht vollständig, aber immerhin so weit aufgelöst wird, dass ein Rückschluss auf eine bestimmte Person nur unter „Hinzuziehung zusätzlicher Informationen“, insbes. eines Identifizierungsschlüssels, möglich ist.

- ☐ Ja
- ☐ Nein

2.6 Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten durch kryptografische Maßnahmen so verändert werden, dass sie – insbes. während ihres Übertragungsvorgangs – ohne den Schlüssel nicht mehr lesbar sind, ein unberechtigter Zugriff Dritter mithin ausgeschlossen ist.

- ☐ Ja
- ☐ Nein

3. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

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.

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Firewall
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Protokollierung von Übermittlungen
- ☐ Erstellen einer Übersicht von Datenträgern, Aus- und Eingang
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☐ Sicherung von Datenträgertransporten (verschließbarer Transportbehälter) auch für Papier

3.2 Eingabekontrolle/Verarbeitungskontrolle

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

- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Protokollauswertungsroutinen/-systeme vorhanden
- ☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

3.3 Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

- ☐ Führung eines Verzeichnisses von Verarbeitungstätigkeiten
- ☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration
- ☐ Zulässigkeit eines Datentransfers in Drittländer ist gegeben

3.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ☐ Vorhandene Vereinbarungen zur Auftragsdatenverarbeitung
- ☐ Kontrolle der Vertragsausführung
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Regelung zu Wartungen (speziell Fernwartung)

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

4.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

☐ Unterbrechungsfreie Stromversorgung (USV)
☐ Überspannungsschutz
☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)
☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
☐ Feuer- und Rauchmeldeanlagen
☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
☐ Testen von Datenwiederherstellung
☐ Klimaanlage in Serverräumen
☐ Schutzsteckdosenleisten in Serverräumen
☐ Feuerlöschgeräte vor den Serverräumen
☐ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
☐ Virenschutzsystem
☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)
☐ Konzept für Katastrophenfall vorhanden

4.2 Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten)

Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

☐ Redundante Systemauslegung
☐ Ausfallsicherheits-/Hochverfügbarkeitskonzept
☐ Einsatz fehlertoleranter Software
☐ Schutz vor Überlast und Denial of Service-Angriffen

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

☐ Datenschutz-Management
☐ Incident-Response-Management
☐ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Wichtiger Hinweis!

Wir müssen darauf hinweisen, dass dieses Muster nur Anhaltspunkte liefern kann und keine anwaltliche Beratung ersetzt. Wir übernehmen keine Haftung für die korrekte Anwendung im Einzelfall und die Aktualität zum Zeitpunkt der Verwendung.
IHK Trier, 25.5.2018