Dokumentation der getroffenen technischen und organisatorischen Maßnahmen für die folgende Verarbeitung personenbezogener Daten:[1]

Nachfolgend wird durch Ankreuzen dargestellt, welche technischen und organisatorischen Maßnahmen bereits getroffen werden, um den Anforderungen der Datenschutz-Grundverordnung (Art. 5, 24, 25 und 32 DS-GVO) zu entsprechen. Bei der Auswahl und Umsetzung der Maßnahmen kommt es im Einzelfall darauf an, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird.[2] Die Aufzählung ist nicht abschließend und kann ergänzt werden. Bei Auftragsverarbeitungen, Vergabe von Unteraufträgen oder Fernwartungsaufträgen sind die Maßnahmen der Auftragsverarbeiter in einer gesonderten Anlage aufzuführen.

☐ Eine Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO wurde durchgeführt.[3]

1. Transparenz

Transparenz im Sinne des Art. 5 Abs. 1 lit. a DS-GVO ist gewährleistet, wenn die Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dazu muss der Verantwortliche gemäß Art. 12 Abs. 1 DS-GVO geeignete Maßnahmen treffen, um den Informations- und Mitteilungspflichten nach Art. 13 und 14 DS-GVO Rechnung tragen und die entsprechenden Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln zu können.

☐ *Dokumentation der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung*

☐ *Dokumentation der Datenempfänger und Zeitspanne der Überlassung*

☐ *Dokumentation der Mandanten und zugehörigen Datenbereiche*

☐ *Dokumentation verbindlicher Löschfristen*

☐ *Dokumentation von Auftrags- und Unterauftragsverhältnissen*

☐ *Veröffentlichung der Dokumentationen (z. B. online)*

☐ *Bereitstellung der hier markierten Dokumentationen auf Antrag der betroffenen Person*

☐ *Veröffentlichung der Informationen zur Verarbeitung von personenbezogenen Daten (z. B. online oder als Aushang) als Datenschutzerklärung*

☐ _____

2. Zweckbindung

Zweckbindung im Sinne des Art. 5 Abs. 1 lit. b DS-GVO ist gewährleistet, wenn die Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

☐ *Darstellung der Zwecke im Verzeichnis von Verarbeitungstätigkeiten*

☐ *Verpflichtung der Mitarbeiter auf die Beachtung der Anforderungen der DS-GVO*

☐ *Erlass einer schriftlichen Dienstanweisung zur Verarbeitung personenbezogener Daten*

☐ *Entgegennehmen ausschließlich schriftlicher Weisungen nur von befugten Mitarbeitern des Verantwortlichen bzw. Auftraggebers*

---

[1] Bitte die Bezeichnung der Datenverarbeitung hier eintragen.

[2] Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere des Risikos der Beeinträchtigung der Rechte und Freiheiten natürlicher Personen müssen gemäß Art. 32 Abs. 1 DS-GVO berücksichtigt werden, um geeignete Maßnahmen nach dem Stand der Technik treffen zu können.

[3] Bitte durch entsprechende Unterlagen dokumentieren.

☐ _____

3. Datenminimierung

Datenminimierung im Sinne des Art. 5 Abs. 1 lit. c DS-GVO ist gewährleistet, wenn die Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind.

☐ *Datenschutz durch Technikgestaltung*[4] *(data protection by design)*

☐ *Vornahme datenschutzfreundlicher Voreinstellungen*[5] *(data protection by default)*

☐ *Plausibilitätskontrollen zur Beschränkung der Datenerhebung*

☐ *Festlegung verbindlicher Löschfristen*[6]

☐ *Regelmäßiges manuelles Auslösen der Löschung nicht benötigter Daten.*

☐ *Festlegung automatisierter Löschzyklen*

☐ *Pseudonymisierung der Daten bei Weiterverarbeitung oder Übermittlung*

☐ *Anonymisierung von Daten wenn Identifikation nicht mehr notwendig*

☐ *Regelmäßige Audits über den Datenumfang (durch die/den Datenschutzbeauftragte(n))*

☐ _____

4. Richtigkeit

Richtigkeit im Sinne des Art. 5 Abs. 1 lit. d DS-GVO ist gewährleistet, wenn die verarbeiteten Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind und Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

☐ *Nachweis der Herkunft von Daten*

☐ *Zertifikatsbasierte Authentifizierung der Datenquelle*

☐ *Nutzung von De-Mail*

☐ *Identitätsprüfung bei Anlieferung von Daten*

☐ *Nutzung des Post-Ident-Verfahrens*

☐ *Nutzung eines Video-Ident-Verfahrens*

☐ *Unverzügliche Löschung unrichtiger Daten*

☐ *Unverzügliche Berichtigung unrichtiger Daten*

☐ *Beantragung einer Berichtigung durch elektronische Antragstellung*

☐ *Einrichtung eines Verfahrens zur Berichtigung von Daten auf Antrag*

☐ *Eigenständige elektronische Berichtigung der Daten durch die betroffene Person*

☐ _____

5. Speicherbegrenzung

Speicherbegrenzung im Sinne des Art. 5 Abs. 1 lit. e DS-GVO ist gewährleistet, wenn die verarbeiteten Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

---

[4] Bereits bei der Planung und Erstellung von Software, Anwendungen und Verfahren werden die Datenschutzgrundsätze des Art. 5 DS-GVO berücksichtigt.

[5] Bei der Konfiguration, Auslieferung und Inbetriebnahme von Software, Anwendungen und Verfahren werden die Datenschutzgrundsätze des Art. 5 DS-GVO berücksichtigt

[6] Bitte durch entsprechende Unterlagen dokumentieren.

☐ *Frühzeitige Anonymisierung personenbezogener Daten*

☐ *Frühzeitige Pseudonymisierung personenbezogener Daten*

☐ _____

6. Vertraulichkeit

Vertraulichkeit im Sinne des Art. 32 Abs 1 lit. b in Verbindung mit ErwGr 39 und 83 DS-GVO ist hinreichend gewährleistet, wenn Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können und die Daten außerdem gemäß Art. 5 Abs. 1 lit. f DS-GVO vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust geschützt sind.

☐ *Alarmanlage*

☐ *Wachpersonal*

☐ *Zugangskontrollsystem*

☐ *Unterteilung in Sicherheitszonen*

☐ *Sicherheitsschlösser*

☐ *Schlüsselregelung*

☐ *Schließsystem mit Chipkarte*

☐ *Schließsystem mit Transponder*

☐ *Schließsystem mit Codesperre*

☐ *Manuelles Schließsystem*

☐ *Biometrische Zugangssperren*

☐ *Ausweispflicht*

☐ *Personenkontrolle*

☐ *Festlegung befugter Personen*

☐ *Einbruchhemmende Fenster und Türen*

☐ *Geräte- und Gehäuseversiegelung*

☐ *Auf Datenschutz verpflichtetes Reinigungspersonal*

☐ *Auf Datenschutz verpflichtetes Wartungspersonal*

☐ *Festgelegte Reinigungszeiten*

☐ *Beaufsichtigung von Wartungstätigkeiten*

☐ *Zugangsbeschränkung nach Endgerät*

☐ *Zeitliche Zugangsbeschränkung*

☐ *Benutzerkonto für jeden Mitarbeiter*

☐ *Implementierung eines Rollen- und Berechtigungskonzepts*[7]

☐ *Arbeiten mit individuellen Benutzerkennungen*

☐ *Dem Zweck angemessene Passwortrichtlinien*[7]

☐ *Regelmäßige Passwortwechsel*

☐ *Single Sign-on*

☐ *Authentifikation mit Passwort*

☐ *Authentifikation mit SmartCard*

☐ *Authentifikation über Verzeichnisdienste*

☐ *Biometrische Authentifikation*

☐ *Regelungen beim Ausscheiden von Mitarbeitern*

☐ *Sperren der Bootkonfiguration (BIOS, UEFI)*

☐ *Automatische Abmeldevorgänge*

☐ *Kontensperrung nach mehrmaliger Falscheingabe des Passworts*

☐ *Aufteilung der Administratorrechte unter verschiedenen Personen*

☐ *Vergabe von Administratorrechten an minimale Anzahl Personen*

☐ *Sicheres Löschen*[8] *von Datenträgern*

☐ *Sicheres Löschen*[8] *einzelner Dateien*

[7] Bitte durch entsprechende Unterlagen dokumentieren.

[8] z. B. Mehrmaliges vollständiges Überschreiben des vorherigen Inhalts mit Zufallswerten

- ☐ *Differenzierung administrativer Aufgaben*
- ☐ *Dateiverschlüsselung*
- ☐ *Datenträgerverschlüsselung*
- ☐ *Verschlüsselung von Datenbanken*
- ☐ *Sperrung der Nutzung von persönlichem Cloud-Speicher am Arbeitsplatz-PC*
- ☐ *Verhinderung nicht-autorisierter Cloud-Synchronisation durch Drittanbietersoftware*[9]
- ☐ *Übermittlung von Daten in anonymisierter Form*
- ☐ *Übermittlung von Daten in pseudonymisierter Form*
- ☐ *Sichere Behältnisse bei physischem Transport*
- ☐ *Zuverlässiges Transportpersonal*
- ☐ *Identitätsnachweis des Transportpersonals*
- ☐ *Datenträgervernichtung nach DIN 66399*
- ☐ *Nach Verarbeitungszweck differenziertes Berechtigungskonzept*
- ☐ *Logische Mandantentrennung*
- ☐ *Physikalisch getrennte Speicherung und Verarbeitung*
- ☐ *Trennung von Produktiv- und Testsystem*
- ☐ *Fernlöschung von mobilen Endgeräten*
- ☐ *E-Mail-Verschlüsselung mit S/MIME*
- ☐ *E-Mail-Verschlüsselung mit OpenPGP*
- ☐ *Durchgängige Transportverschlüsselung bei der E-Mail-Übertragung*
- ☐ *Transportverschlüsselte Datenübertragung*
- ☐ *Datenkommunikation über VPN-Tunnel*
- ☐ _____

7. Integrität

Integrität im Sinne des Art. 32 Abs 1 lit. b in Verbindung mit Art. 5 Abs. 1 lit. f DS-GVO ist gewährleistet, wenn Daten vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sind, die Daten also vollständig, unverändert und unversehrt[10] sind.

- ☐ *Signieren elektronischer Dokumente*
- ☐ *Signieren von E-Mails*
- ☐ *Anwendung von Prüfsummenverfahren*
- ☐ *Überwachung von Fernwartungsaktivitäten*
- ☐ *Sperren externer Schnittstellen wie USB*
- ☐ *Intrusion Detection System*
- ☐ *Einsatz von Virenschutzlösungen*
- ☐ *Application Layer Firewall*
- ☐ *E-Mail-Signierung mit S/MIME*
- ☐ *E-Mail-Signierung mit OpenPGP*
- ☐ *Verschlüsselung der Internetpräsenz*
- ☐ *Packet Filter Firewall*
- ☐ *Dedizierte Netze für Systeme mit sensiblen Daten*
- ☐ *Automatisierte Updateprozesse für Betriebssysteme, Anwendungen und Dienste*

[9] Jede Nutzung von Cloud-Diensten bei der Verarbeitung personenbezogener Daten muss als Auftragsverarbeitung gemäß Art. 28 DS-GVO gestaltet werden.

[10] Siehe dazu auch Glossar des IT-Grundschutz-Kompendiums des Bundesamtes für Sicherheit in der Informationstechnik BSI (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html)

- ☐ *Differenzierte Berechtigungen für unterschiedliche Transaktionen*
- ☐ *Differenzierte Berechtigungen für Datenobjekte*
- ☐ *Plausibilitätskontrollen bei der Datenverarbeitung*
- ☐ *Inhaltsverschlüsselte Datenübertragung*
- ☐ *Regelung zum Umgang mit mobilen Datenträgern*
- ☐ *Verschlüsselung von mobilen Datenträgern*
- ☐ *E-Mail-Gateway mit Filterfunktion*
- ☐ _____

8. Verfügbarkeit

Verfügbarkeit im Sinne des Art. 32 Abs. 1 lit. b DS-GVO ist gewährleistet, wenn die Daten ihrem Zwecke nach jederzeit nutzbar sind. Zusätzlich muss gemäß Art. 32 Abs. 1 lit. c DS-GVO die Fähigkeit existieren die Verfügbarkeit und den Zugang zu den Daten bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können.

- ☐ *Sicherungs- und Wiederherstellungskonzept (Backup & Recovery)*
- ☐ *Automatisiertes Anfertigen von Datensicherungen (Backup)*
- ☐ *Aufbewahrung von Datenträgern in gegen Elementarschäden gesicherten Behältnissen*
- ☐ *Aufbewahrung der Datensicherung in einem anderen Brandabschnitt*
- ☐ *Festgelegte Zuständigkeiten für die Datensicherung*
- ☐ *Regelmäßiger Test der Datenwiederherstellung*
- ☐ *Notfallplan zur Wiederinbetriebnahme von Servern und Diensten*
- ☐ *Datenträgerspiegelung (RAID)*
- ☐ *Datenreplikation*
- ☐ *Vermeidung lokaler Datenspeicherung*
- ☐ *Notfallplan bei Kompromittierung*
- ☐ *Notfallplan bei Datenverlust*
- ☐ *Redundante IT-Systeme*
- ☐ *Virtualisierte Infrastruktur*
- ☐ *Automatisches Benachrichtigungssystem bei Ausfall*
- ☐ _____

9. Belastbarkeit

Belastbarkeit ist gemäß Art. 32 Abs. 1 lit. b auf Dauer sicherzustellen und betrifft Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

- ☐ *Lastausgleich (load balancing) der Netzwerkkomponenten*
- ☐ *Lastausgleich (load balancing) der Server*
- ☐ *Lastausgleich (load balancing) der Dienste*
- ☐ *Automatische Skalierung virtueller Systeme*
- ☐ *Unterbrechungsfreie Stromversorgung*
- ☐ *Überspannungsschutz*
- ☐ *Klimaanlage in Serverräumen*
- ☐ *Feuer- und Rauchmeldeanlagen*
- ☐ *Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen*
- ☐ *Feuerlöscher / automatisches Löschsystem*
- ☐ *Automatisches Benachrichtigungssystem bei Erreichung der max. Auslastung*
- ☐ *IT-Komponenten verfügen über erforderliche Leistungsfähigkeit*
- ☐ *Schutz vor Wassereinbruch*
- ☐ *Schutz vor Hochwasser*

☐ *Automatisches Notrufsystem*

☐ *Eignung der Räumlichkeiten / des Baus*

☐ _____

10. Rechenschaftspflicht und Wirksamkeitsnachweis

Rechenschaftspflicht im Sinne des Art. 5 Abs. 2 DS-GVO ist erfüllt, wenn der Verantwortliche die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen kann. Unabhängig davon muss er gemäß Art. 32 Abs. 1 lit. d DS-GVO in der Lage sein, die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig überprüfen, bewerten und evaluieren zu können. Außerdem muss er gem. ErwGr 87 DS-GVO sofort feststellen können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können.

☐ *Führen eines Verzeichnisses von Verarbeitungstätigkeiten*

☐ *Bestellung eine(r/s) Datenschutzbeauftragten*

☐ *Dokumentation über vorhandene IT-Infrastruktur*

☐ *Dokumentation über eingesetzte Programme und Anwendungen*

☐ *Dokumentation der getroffenen Sicherheitsmaßnahmen (im Verzeichnis von Verarbeitungstätigkeiten)*

☐ *Dokumentation der Vernichtung oder Rückgabe von Datenträgern und Unterlagen nach Beendigung eines Auftrags*

☐ *Protokollierung der Anmeldevorgänge*

☐ *Protokollierung der Datenzugriffe*

☐ *Protokollierung gescheiterter Zugriffsversuche*

☐ *Sicherung der Protokolldaten gegen Veränderung und Verlust*

☐ *Automatisierte Auswertung der Protokolldaten*

☐ *Protokollierung der Datenträgervernichtung*

☐ *Protokollierung von Löschvorgängen*

☐ *Protokollierung der Übermittlungsvorgänge*

☐ *Videoüberwachung bei Zutritt zur Datenverarbeitungsanlage*

☐ *Benutzerkennungsbezogene Protokollierung*

☐ *Dokumentation der Übergabeprozesse bei physischem Transport von Datenträgern*

☐ *Protokollierung des Zutritts zu Datenverarbeitungsanlagen oder Räumen in denen Datenverarbeitung stattfindet*

☐ *Protokollierung aller Administratorenaktivitäten*

☐ *Protokollierung der Eingabe bei der Erhebung und Ergänzung von Daten*

☐ *Protokollierung der Veränderung oder Korrektur von gespeicherten Daten*

☐ *Protokollierung der sicheren Löschungen von Datenträgern*

☐ *Stichprobenartige Überprüfung der Wirksamkeit bestimmter Maßnahmen*[11]

☐ _____

[11] Bitte durch entsprechende Unterlagen dokumentieren.