Anlage 1

Technische und organisatorische Maßnahmen zu § 11 des Auftragsdatenverarbeitungsvertrages

Gemäß § 11 des Auftragsdatenverarbeitungsvertrages muss der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Im Vertrag sind insbesondere die technischen und organisatorischen Maßnahmen, welche die Datensicherheit gewährleisten, schriftlich festzulegen. Aus den IT-Grundschutz-Katalogen des BSI können einzelne Maßnahmen in den Vertrag übernommen werden, soweit es sich um einen normalen Schutzbedarf handelt. Die IT-Grundschutz-Kataloge sind jedoch nicht abschließend. Insbesondere bei der Verarbeitung personenbezogener Daten besonderer Art sind in der Regel zusätzliche Maßnahmen erforderlich.

Die nachfolgend festgelegten technischen und organisatorischen Maßnahmen bei der automatisierten Datenverarbeitung werden vom Auftragnehmer umgesetzt, um diese Schutzziele zu erreichen.[1]

1. Vertraulichkeit

Vertraulichkeit ist gewährleistet, wenn die gespeicherten Daten nicht in die Hände Unbefugter geraten können, was durch folgende Maßnahmen realisiert werden kann:

- ☐ *Alarmanlage*
- ☐ *Zugangskontrollsystem*
- ☐ *Sicherheitsschlösser*
- ☐ *Schließsystem mit Chipkarte*
- ☐ *Schließsystem mit Codesperre*
- ☐ *Biometrische Zugangssperren*
- ☐ *Personenkontrolle*
- ☐ *Festlegung befugter Personen*
- ☐ *Fensterversiegelung*
- ☐ *Auf Datenschutz verpflichtetes Reinigungs- und Wartungspersonal*
- ☐ *Beaufsichtigung der Reinigung und Wartung*
- ☐ *Benutzerkonto für jeden Mitarbeiter*
- ☐ *Zugangsbeschränkung nach Endgerät*
- ☐ *Wachpersonal*
- ☐ *Videoüberwachung*
- ☐ *Schlüsselregelung*
- ☐ *Schließsystem mit Transponder*
- ☐ *Manuelles Schließsystem*
- ☐ *Ausweispflicht*
- ☐ *Protokollierung des Zutritts*
- ☐ *Unterteilung in Sicherheitszonen*
- ☐ *Sperren von BIOS und Bootmedien*
- ☐ *Festgelegte Reinigungs- und Wartungszeiten*
- ☐ *Geräte- und Gehäuseversiegelung*
- ☐ *Zeitliche Zugangsbeschränkung*
- ☐ *Regelungen bei Ausscheiden von Mitarbeitern*

[1] Zutreffendes bitte ankreuzen und ggf. durch weiter Unterlagen dokumentieren.

- ☐ *Automatische Abmeldevorgänge*
- ☐ *Kontensperrung nach mehrmaliger Falscheingabe des Passworts*
- ☐ *Aufteilung der Administratorrechte unter verschiedenen Personen*
- ☐ *Vergabe von Administratorrechten an minimale Anzahl Personen*
- ☐ *Sicheres Löschen[5] von Datenträgern*
- ☐ *Sicheres Löschen[2] einzelner Dateien*
- ☐ *Protokollierung von Löschvorgängen*
- ☐ *Verschlüsselung von Datenbanken*
- ☐ *Datenträgervernichtung nach DIN 66399*
- ☐ *Protokollierung der Datenträgervernichtung*
- ☐ *Sperrung der Nutzung von persönlichem Cloud-Speicher am Arbeitsplatz-PC*
- ☐ *Verhinderung nicht-autorisierter Cloud-Synchronisation durch Drittanbietersoftware[3]*
- ☐ *Weitergabe von Daten in anonymisierter Form*
- ☐ *Weitergabe von Daten in pseudonymisierter Form*
- ☐ *Sichere Behälter und Verpackungen bei physischem Transport*
- ☐ *Zuverlässiges Transportpersonal*
- ☐ *Identitätsnachweis des Transportpersonals*
- ☐ *Dokumentation der Übergabeprozesse bei physischem Transport*
- ☐ *Berechtigungskonzept mit gesonderten Eingabe-, Änderungs- und Löschbefugnissen*
- ☐ *Fernlöschung von mobilen Endgeräten*
- ☐ *Arbeiten mit individuellen Benutzerkennungen*
- ☐ *Benutzerkennungsbezogene Protokollierung*
- ☐ *Protokollierung aller Administratorenaktivitäten*
- ☐ *Logische Mandantentrennung*
- ☐ *Physikalisch getrennte Speicherung und Verarbeitung*
- ☐ *Trennung von Produktiv- und Testsystem*
- ☐ *Differenzierte Berechtigungen bei der Datenverwaltung*
- ☐ *Differenzierung administrativer Aufgaben bei der Datenverwaltung*
- ☐ *……...*
- ☐ *……...*

2. Integrität

Integrität ist gewährleistet, wenn Datenbestände unversehrt, vollständig und aktuell, also verlässlich richtig sind. Sie muss während der Erhebung und allen Phasen der Verarbeitung gegeben sein und kann durch folgende Maßnahmen realisiert werden:

- ☐ *Authentifikation mit Passwort*
- ☐ *Authentifikation mit SmartCard*
- ☐ *Authentifikation über Verzeichnisdienste*
- ☐ *Biometrische Authentifikation*
- ☐ *Single Sign On*
- ☐ *Überwachung von Fernwartungsaktivitäten*

[2] Mehrmaliges vollständiges Überschreiben des vorherigen Inhalts mit Zufallszahlen
[3] Jede Nutzung von Cloud-Diensten bei der Verarbeitung personenbezogener Daten muss als Auftragsdatenverarbeitung gestaltet werden.

- ☐ *Sperren externer Schnittstellen wie USB*
- ☐ *Virenschutzlösungen*
- ☐ *Packet Filter Firewall*
- ☐ *Dedizierte Netze für sensible Systeme*
- ☐ *Differenzierte Berechtigungen für unterschiedliche Transaktionen/Funktionen*
- ☐ *Strenge Passwortrichtlinien*
- ☐ *Datenträgerverschlüsselung*
- ☐ *Protokollierung der Dateneingaben*
- ☐ *Protokollierung der Datenlöschungen*
- ☐ *……...*
- ☐ *Intrusion Detection System*
- ☐ *Application Layer Firewall*
- ☐ *Rollenkonzept*
- ☐ *Berechtigungskonzept*
- ☐ *Differenzierte Berechtigungen für Datenobjekte*
- ☐ *Regelmäßige Passwortwechsel*
- ☐ *Dateiverschlüsselung*
- ☐ *Protokollierung der Datenänderungen*
- ☐ *……...*

3. Verfügbarkeit

Verfügbarkeit liegt vor, wenn Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet oder genutzt werden können. Die Verfügbarkeit bezieht sich nicht nur auf die gespeicherten personenbezogenen Daten im engeren Sinne, sondern gleichermaßen auf die Hardware und die zur Verarbeitung erforderlichen Programme. Nur Berechtigte können die ihnen freigegebenen personenbezogene Daten verarbeiten und nutzen, währenddessen Unbefugte diese Daten weder lesen noch verändern können. Um eine hohe Verfügbarkeit zu gewährleisten, können folgende Maßnahmen ergriffen werden:

- ☐ *Einbruchhemmende Fenster*
- ☐ *Sicherungs- und Wiederherstellungskonzept (Backup & Recovery)*
- ☐ *Festgelegte Zuständigkeiten für die Datensicherung*
- ☐ *Notfallplan*
- ☐ *Redundante IT-Systeme*
- ☐ *Unterbrechungsfreie Stromversorgung*
- ☐ *Klimaanlage in Serverräumen*
- ☐ *Sichere Aufbewahrung von (Wechsel-)Datenträgern*
- ☐ *Aufbewahrung der Datensicherung in einem anderen Brandabschnitt*
- ☐ *Regelmäßiger Test der Datenwiederherstellung*
- ☐ *Datenträgerspiegelung (RAID)*
- ☐ *Virtualisierte Infrastruktur*
- ☐ *Überspannungsschutz*
- ☐ *Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen*

- ☐ *Feuer- und Rauchmeldeanlagen*
- ☐ *Feuerlöscher / automatisches Löschsystem*
- ☐ *Automatisches Benachrichtigungssystem*
- ☐ *Automatisches Notrufsystem*
- ☐ *Schutz vor Wassereinbruch und Hochwasser*
- ☐ *Nachweis der Eignung der Räumlichkeiten und Bausubstanz*
- ☐ *……...*
- ☐ *……...*

4. Authentizität

Die Authentizität ist hauptsächlich bei elektronisch übertragenen Dokumenten bedroht. Dem kann durch Verfahren begegnet werden, bei denen die Herkunft der Daten nachvollziehbar ist.

- ☐ *Datenkommunikation über VPN-Tunnel*
- ☐ *Transportverschlüsselte Datenübertragung*
- ☐ *Inhaltsverschlüsselte Datenübertragung*
- ☐ *E-Mail-Verschlüsselung mit PGP*
- ☐ *E-Mail-Verschlüsselung mit S/MIME*
- ☐ *Nutzung von DE-Mail*
- ☐ *Datenerfassungsanweisungen*
- ☐ *Plausibilitätskontrollen*
- ☐ *Identitätsprüfung bei Anlieferung von Daten*
- ☐ *……...*
- ☐ *……...*

5. Revisionsfähigkeit

Revisionsfähig sind Daten, wenn nachprüfbar ist, wie Daten in einen Datenbestand gelangt sind und welche Veränderungen sie im Laufe der Zeit erfahren haben. Nachprüfbar muss sein, wer für das Aufnehmen bestimmter Daten in einen Datenbestand oder ihr Entfernen daraus die Verantwortung trägt.

- ☐ *Protokollierung der Anmeldevorgänge*
- ☐ *Protokollierung der Datenzugriffe*
- ☐ *Protokollierung gescheiterter Zugriffsversuche*
- ☐ *Sicherung der Protokolldaten gegen Veränderung und Verlust*
- ☐ *Automatisierte Auswertung der Protokolldaten*
- ☐ *Übersicht der Anwendungen mit Eingabe-, Änderungs- und Löschfunktion*
- ☐ *Attributierung von Datensätzen nach Zweck der Verarbeitung*
- ☐ *Aufbewahrung der Originaldokumente, deren Daten automatisiert verarbeitet werden*
- ☐ *……...*
- ☐ *……...*

6. Transparenz

Automatisierte Verfahren sind in aktueller Form nachvollziehbar zu dokumentieren. Die einzelnen Verfahrensschritte müssen dabei so beschrieben werden, dass die systematische Richtigkeit der Prozesse nachvollziehbar wird.

- ☐ *Protokollierung der Übermittlungsvorgänge*
- ☐ *Dokumentation der getroffenen Sicherheitsmaßnahmen*
- ☐ *Dokumentation und Auskunft über eingesetzte Programme*
- ☐ *Verpflichtung der Mitarbeiter auf das Datengeheimnis nach § 8 Auftragsdatenverarbeitungsvertrag*
- ☐ *Duldung und Unterstützung von Prüfungen durch den Auftraggeber*
- ☐ *Vertragsstrafen vereinbart*
- ☐ *Vernichtung von Daten nach Beendigung des Auftrags*
- ☐ *Rückgabeverfahren für nicht weiter benötigte Unterlagen*
- ☐ *……...*
- ☐ *Dokumentation der Datenempfänger und Zeitspanne der Überlassung*
- ☐ *Bestellung einer/eines betrieblichen Datenschutzbeauftragten*
- ☐ *Dokumentation und Auskunft über vorhandene IT-Infrastruktur*
- ☐ *Entgegennehmen ausschließlich schriftlicher Weisungen von befugten Mitarbeitern des Auftraggebers*
- ☐ *Wirksame Kontrollrechte für den Auftraggeber vereinbart*
- ☐ *Verbindliche Löschfristen vereinbart*
- ☐ *Vertragliche Regelung des Einsatzes von Unterauftragnehmern*
- ☐ *Dokumentation der Mandanten und zugehörigen Datenbereiche*
- ☐ *……...*

Bitte kreuzen Sie diejenigen Maßnahmen an, die von Ihnen als Auftragnehmer umgesetzt werden. Es müssen Maßnahmen in jedem Themenbereich umgesetzt werden. Bei Vergabe von Unteraufträgen oder Fernwartungsverträgen sind die Maßnahmen des Unterauftragnehmers, falls abweichend von oben genannten, in einer gesonderten Anlage aufzuführen.