Anlage zum Vertrag zur Auftragsdatenverarbeitung

Anforderungen an die technischen und organisatorischen Maßnahmen des Auftragnehmers

1 Gesetzliche Grundlagen zu technisch organisatorischen Maßnahmen

1.1 § 9 BDSG – „Technische und organisatorische Maßnahmen“

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1.2 Anlage zu § 9 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die geeignet sind:

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu 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 von personenbezogenen Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. (Trennungsgebot)

2 Zutrittskontrolle

Zutrittskontrolle

Ziel ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. Hiermit ist der räumliche Zugang zu den Anlagen gemeint.

Umzusetzende Maßnahmen

Zutrittskontrolle des Gebäudes Tag/Nacht

- z.B. Ausweise ohne/mit Foto, Codeschloss, Neutrale Karten / Schlüssel
- Dokumentation der Vergabe von Schlüsseln oder Karten?

Besucherkontrolle

- z.B. durch Besucherbuch, Besucherausweis
- Begleitung durch Mitarbeiter?

Schutzmaßnahmen des Gebäudes Tag/Nacht

- z.B. durch Wachpersonal (intern /extern), Alarmanlage
- Schutz von Außenfenstern und Außentüren?
- Sicherheitsschlösser

Zutrittskontrolle für den Serverraum?

- Mit Protokollierung

Sonstiges

3 Zugangskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -verfahren gehindert werden. Diese beziehen sich – im Gegensatz zur Zutrittskontrolle – auf das Eindringen unbefugter Personen in das EDV-System selbst.

Umzusetzende Maßnahmen

Schriftliche Regelungen für die Nutzung von Datenträgern und Notebooks

- Prüfung der Einhaltung der Regelungen

Verschlüsselung von Notebooks, USB Sticks und von sonstigen mobilen Datenträgern auf denen sich Daten des Auftraggebers befinden

- zentrale Schlüsselverwaltung für verschlüsselte Systeme

Kontrollierte Vernichtung von Datenträgern und elektronischen Daten des Auftraggebers

- Einsatz datenschutzkonformer Verträge
- Einsatz sicherer Löschrprogramme

Zugang zu Daten des Auftraggebers durch Dritte ausschließen

Sonstiges:

4 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass die bei der Bearbeitung verwendeten personenbezogenen Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Umzusetzende Maßnahmen

Schriftliches Berechtigungskonzept des Auftragnehmers

- Schriftliche Dokumentation der Berechtigungsvergabe
- regelmäßige Prüfung bestehender Berechtigungen
- Umsetzung Need-to-know Prinzip

Protokollierung Dateizugriff

- Dokumentation der Dateiänderungen
- Kontrolle der Protokolle

Protokollierung Datenbankzugriff

- Dokumentation der Änderungen
- Kontrolle der Protokolle

Sonstiges

5 Weitergabekontrolle

Maßnahmen, die sicherstellen, 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.

Umzusetzende Maßnahmen

Art der Übertragung von Daten des Auftraggebers wird festgelegt auf

- Wechseldatenträger verschlüsselt, Mail verschlüsselt, Kurierdienst
- Weiter vereinbarte Möglichkeit:

.....

Protokollierung der Datenübertragung

- Automatische Eskalation bei Sicherheitsmeldungen

Schriftliche Regelungen zur Vernichtung / Rückgabe von Datenträgern des Auftraggebers

- In Auftrag
- Folgende Regelung:.....

Benötigen Sie Unterstützung bei der Festlegung der technischen und organisatorischen Maßnahmen

Fernzugriff auf Daten des Auftraggebers durch welche Dritte wird wie besonders geschützt

- Administratoren
Erlaubt ja / nein Schutz vereinbart.....
- Externe Dienstleister?
Erlaubt ja / nein Schutz vereinbart.....

Sonstiges

6 Eingabekontrolle

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

Umzusetzende Maßnahmen

Veränderung / Erfassung von Daten des Auftraggebers

- Eine nachvollziehbare Dokumentation muss erstellt werden (wer, was, wann)

Eine schriftliche Dokumentation der Verfahren bei denen Daten des Auftraggebers verarbeitet werden muss erstellt werden

- Übergabe der Dokumentation in welcher Form:
- Kontrolle der Einhaltung durch Auftragnehmer:.....

Regelmäßige Protokollkontrolle und –auswertungen bei Änderungen an Daten des Auftraggebers

- Automatische Eskalation bei Sicherheitsmeldungen notwendig

Sonstiges:

7 Auftragskontrolle

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

Umzusetzende Maßnahmen

Authentisierung bei Aufträgen des Auftraggebers erfolgt wie folgt:

- Nur schriftliche Aufträge
- Nur wenn Auftraggeber persönlich bekannt und schriftlich bestätigt wird
- Oder:.....

Subunternehmer des Auftragnehmers nur nach ausdrücklicher Genehmigung

- Folgende Subunternehmer sind erlaubt: Sie gesonderte Anlage
- Regelungen mit Subunternehmer mindestens so restriktiv, wie die des Auftraggebers

Kontrollrechte des Auftraggebers beim Subunternehmer des Auftragnehmers

- Kontrollrechte des Auftraggebers in den Vertrag zwischen Auftragnehmer und dessen Subunternehmer ist aufzunehmen

Sonstiges:

8 Verfügbarkeitskontrolle

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

Umzusetzende Maßnahmen

Ein ausreichender Virenschutz ist umzusetzen

- Ein schriftliches Virenschutzkonzept ist nachzuweisen

Ein ausreichender Firewallschutz ist umzusetzen.

- Ein schriftliches Firewallkonzept ist nachzuweisen
- Eine detaillierte Dokumentation der Firewall ist nachzuweisen

Ein schriftliches Datensicherungskonzept und eine Dokumentation der Datensicherung ist nachzuweisen

- Daten des Auftraggebers sollen durch die Datensicherung erfasst werden ?

ja / Nein

Anzahl der zu erstellenden Datensicherungsgenerationen

- Anzahl:.....Sicherung per Band / Snapshot

Regelmäßig Rücksicherungen sind zu testen und zu dokumentieren?

- Vereinbarte Zeitintervalle.....

Unterbrechungsfreie Stromversorgung ist einzusetzen und zu testen

Lagerung und Dokumentation der Datenträger der Datensicherung:

- Sichere Aufbewahrung in anderem Brandabschnitt vereinbart? Ja / Nein
- Sichere Entsorgung nachzuweisen Ja / Nein

Einsatz von Feuerschutzmaßnahmen oder Früherkennung ist notwendig

- Maßnahmen nachzuweisen Ja / Nein

Einsatz von Sicherheitsupdates auf Systemen auf denen Daten des Auftraggebers verarbeitet werden ist notwendig

- Umsetzung nachzuweisen Ja / Nein?

Bestehen Notfallplan eines Notfallplans ist notwendig

- Umsetzung nachzuweisen Ja / Nein?

Sonstiges

9 Trennungsgebot

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

Umzusetzende Maßnahmen
Trennung der Daten des Auftraggebers von eigenen Daten / anderen Auftragsdaten hat zu erfolgen <ul style="list-style-type: none">• Durch physikalische Trennung oder• Trennung im Rahmen des Berechtigungskonzepts
Trennung von Entwicklungs-, Test- und Produktivsystem hat zu erfolgen <ul style="list-style-type: none">• Trennung durch anderes Netzsegment hat zu erfolgen• Umsetzung nachzuweisen Ja / Nein?
Sonstiges

10 Auftragspezifische Zusatzmaßnahmen