EDV Sachverständigenbüro
Michael J. Schüssler
Wirtschaftsinformatiker
EDV Sachverständiger &
Externer Datenschutzbeauftragter
Hanauer Strasse 71
63741 Aschaffenburg
Tel.: 06021 / 439 18 45
Email: info@svb-ms.de
www.Datenschutz4You.com

DATEN-SCHUTZ

§ 9 plus Anlage BDSG.

Dokumentation der.

technischen und organisatorischen Maßnahmen.

Unternehmen:
Firma
Straße
PLZ ORT

GEPRÜFTES DATEN-SCHUTZ § 11 BDSG UNTERNEHMEN

EDV Sachverständigen- und Datenschutzbüro M. Schüssler.

Wir sind nach ISO/IEC 27001 Foundation ISMS und als externe Datenschutzbeauftragte

gemäß § 4f Abs. 2 S. 1 BDSG zertifiziert.

ANSCHRIFT

Hanauer Straße 71

63741 Aschaffenburg

Tel.: 06021 / 439 18 45

Mobil: 0179 / 49 68 941

E-Mail: info@svb-ms.de

Internet: www.datenschutz4you.com

TÜV SÜD ISO 27001

Bei Rückfragen steht Ihnen unser EDV Sachverständigenbüro sehr gerne zur Verfügung.

IT-Sicherheitsziele(§9 plus Anl. Nr. 1 bis 3 BDSG)

Zutrittskontrolle, Nr.1.
Gebäude, Serverräume…

Zugangskontrolle, Nr. 2
Authentifikation

Zugriffskontrolle, Nr. 3
Berechtigungskonzept

ACCESS DENIED / ACCESS ALLOWED ?

Normative Anforderungen
Grundwerte der Informations-sicherheit.

Erwartungen / Ergebnisse

Verfügbarkeit

Vertraulichkeit

Integrität

Informationen (Assets)

Login
Passwörter
Zugangs-Codes
Zugriffs-Codes
Personen bezogene Daten
Unternehmensdaten
Kundenstamm
Lieferantenstamm
Personalstamm…

Authentizität

Zurechenbarkeit

Verbindlichkeit

Verlässlichkeit

SSL, VPN….	Protokolldatei Logfiles…	Gemäß §11 BDSG	Backup, Recovery…	Gemäß §9 plus Anlage
Weitergabe-kontrolle(4)	**Eingabe-kontrolle(5)**	**Auftrags-kontrolle(6)**	**Verfügbarkeits-kontrolle(7)**	**Zwecktrennungs-gebot(8)**

IT-Sicherheitsziele (§9 plus Anl. Nr. 4 bis 8 BDSG)

Präambel - Datenschutz Aktivitäten

1. In unserem Unternehmen werden ständig automatisiert personenbezogen Daten, durch:

   Weniger als 10 ☐ mehr als 9 ☐ Personen verarbeitet.

2. Von unserem Unternehmen wurde ein Datenschutzbeauftragter schriftlich bestellt.

   Ja ☐ am: _____, der Fachkundenachweis gemäß § 4f Abs. 2 Satz1(BDSG), liegt vor.

   Ja ☐ Nein ☐

   Name und _____

   Anschrift des DSB _____

3. Unsere Mitarbeiter wurden im Datenschutz geschult.

   Ja ☐ am: _____Nein ☐

4. Unser Unternehmen führt folgende Verfahrensverzeichnisse.

   Ja ☐ Nein ☐

   Verfahrensverzeichnisse-Übersicht(sortiert nach Namen)

   1. _____, erstellt am: _____
   2. _____, erstellt am: _____
   3. _____, erstellt am: _____
   4. _____, erstellt am: _____
   5. _____, erstellt am: _____
   6. _____, erstellt am: _____
   7. _____, erstellt am: _____

§ 9 Technische und organisatorische Maßnahmen(BDSG)

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.

Im folgendem sind die technischen und organisatorischen Maßnahmen unseres Unternehmens gemäß § 9 plus Anlage(BDSG), dokumentiert.

Bei eindeutigen Verfahren oder Maßnahmen(unter allgemeine Beschreibung) reicht eine stichwortartige Benennung des Verfahrens z.B. („SSLv3“) aus. Bei Maßnahmen welcher einer Erläuterung bedürfen z.B. „Videoüberwachung“, sollte auch beschrieben werden welche Räume überwacht werden. Auch bei „Passwortverfahren“ ist es z. B. hilfreich, wenn Sie die Mindestpasswortlänge, die Passwortkomplexität und den Passwortänderungszeitraum mit angeben.

Alle Beschreibungen bzw. Daten dienen ausschließlich der Erhebung und der Feststellung der Datenschutz-Qualität unseres Unternehmens gemäß § 9 plus Anlage (BDSG). Die Daten werden nur für den Zweck für welchen sie erhoben wurden verarbeitet und werden streng vertraulich behandelt.

1. Zutrittskontrolle gemäß § 9 plus Anlage Nr. 1

Gemeint sind Maßnahmen um zu verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden - Gebäudesicherung, Räume Sicherung.

Regelung der Zutrittskontrolle

Gebäudesicherung

- Personenkontrolle beim Pförtner / Empfang ☐
- Protokollierung der Besucher ☐
- Tragepflicht von Besucher und -Berechtigungsausweisen ☐
- Videoüberwachung des Hauseingangs ☐
- Ist die Videoüberwachung gekennzeichnet ☐
- Alarmanlagen ☐
-

Sicherung der Räume

- Sicherheitsschlösser ☐
- Schlüsselregelung (Schlüsselausgabe etc.) ☐
- Biometrische Benutzeridentifikation(z. B. Fingerabdruck) ☐
- Chipkartenleser ☐
- Codeschlösser ☐
- Sicherheitsverglasung ☐
- Abschließbare Serverkäfige(Protokollierung der Zutritte) ☐
- Lichtschranken / Bewegungsmelder ☐

Zutrittskontrolle

Allgemeine Beschreibung der Zutrittskontrolle:

2. Zugangskontrolle gemäß § 9 plus Anlage Nr. 2

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

Regelung der Zugangskontrolle

- Komplexe Passwortvergabe ☐
- Authentifikation mit biometrischen Verfahren ☐
- Authentifikation mit Benutzername / Passwort ☐
- Zuordnung von Benutzerrechten ☐
- Erstellen von Benutzerprofilen ☐
- Zuordnung von Benutzerprofilen zu IT-Systemen ☐
- Gehäuseverriegelungen ☐
- Einsatz von VPN-Technologie ☐
- Einsatz von SSL-Verschlüsselung und Zertifikaten ☐
- Sperren von externen Schnittstellen (USB etc.) ☐
- Sperren von offenen Netzwerkverbindungen ☐
- Einsatz von Intrusion Detection System (IDS) ☐
- Verschlüsselung von mobilen Datenträgern ☐
- Verschlüsselung von Smartphone-Inhalten ☐
- Einsatz von Anti-Viren-und Software ☐
- Verschlüsselung von Datenträgern in Laptops / Notebooks ☐
- Einsatz von Hardware-Firewall ☐
- Einsatz von Software-Firewall ☐
- LAN durch DMZ vom Internet separiert ☐
- Kritische Ports in Domain-Umgebung sind gesichert(z.B. 135) ☐
- WPA2, NAT und integrierte Firewall für Router aktiv ☐

Zugangskontrolle

Allgemeine Beschreibung der Zugangskontrolle:

3. Zugriffskontrolle gemäß § 9 plus Anlage Nr. 3

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.

Regelung der Zugriffskontrolle

- Zugriffsberechtigungskonzept vorhanden ☐
- Verwaltung der Rechte durch Systemadministrator ☐
- Systemadmins wurden im Datenschutz geschult ☐
- Systemadmins wurden auf das Datengeheimnis verpflichtet ☐
- Die bes. Zweckbindung gemäß § 31 BDSG ist diesen bekannt ☐
- Passwortrichtlinie und Passwortwechsel sind Mitarbeitern bekannt ☐
- Protokollierung der Zugriffe(Logfiles) ☐
- Backupkonzept ist vorhanden(z.B. Großvater-Vater-Sohn Prinz.) ☐
- Sichere Aufbewahrung von Datenträgern ist gewährleistet ☐
- physische Löschung von Datenträgern vor Wiederverwendung ☐
- ordnungsgemäße Vernichtung von Datenträgern(DIN 32757) ☐
- Protokollierung der Vernichtung ☐
- Verschlüsselung von Datenträgern ☐

Zugriffskontrolle

Allgemeine Beschreibung der Zugangskontrolle:

4. Weitergabekontrolle gemäß § 9 plus Anlage Nr. 4

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.

Regelung der Weitergabekontrolle

- E-Mail-Verschlüsselung ☐
- Einsatz von digitalen Signaturen ☐
- Verschlüsselung der Datenträgern ☐
- Die Weitergabe von besonderen Arten von pbD gemäß§ 3 Abs. 9 (BDSG), erfolgt in anonymisierter oder pseudonymisierter Form ☐
- Weitergabe per SFTP-Servers ☐
- Detaillierte Protokollierungs- und Protokollauswertungssysteme vorh. ☐
- Die Zurechenbarkeit und Verbindlichkeit ist gegeben ☐
- Dokumentation der Empfänger von Daten ☐
- Bei der Datenübermittlung ins Ausland wird die Richtlinie 95/46/EG des Europäischen Parlaments beachtet ☐
- Benutzung sicherer Transportbehälter (Versiegelung) ☐
- Übergabe erfolgt gegen Quittung ☐

Weitergabekontrolle

Allgemeine Beschreibung der Zugangskontrolle:

5. Eingabekontrolle gemäß § 9 plus Anlage Nr. 5

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

Über die Werkzeuge der Nutzerverwaltung und der damit verbundenen Rechteverwaltung muss nachvollziehbar sein, wer Neueingaben, Änderungen oder das Löschen personenbezogener und vertraulicher Informationen veranlasst hat.

Regelung der Eingabekontrolle

- Gibt es einen Dateiverantwortlichen(Owner) ☐
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts ☐
- Protokollierung der Eingabe, Änderung und Löschung von Daten ☐
- Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch Speicherung der ID, Benutzername, Datum, Anlass etc. ☐
- Einsatz von Logfiles ☐
- Gibt es eine Applikationsübersicht, aus welcher hervorgeht, welche Daten eingegeben, geändert und gelöscht werden können. ☐

Eingabekontrolle

Allgemeine Beschreibung der Zugangskontrolle:

6. Auftragskontrolle gemäß § 9 plus Anlage Nr. 6

Die verantwortliche Stelle bedient sich im Falle von § 11 einer anderen Stelle, die für sie im Auftrag und weisungsabhängig personenbezogene Daten erhebt, verarbeitet oder nutzt. Die Auftrag gebende Stelle bleibt im vollen Umfang für den Umgang mit ihren personenbezogenen Daten beim Dienstleister verantwortlich. Datenbewegungen zwischen Auftraggeber und Auftragnehmer stellen keine Datenübermittlungen im Sinne des BDSG dar (vgl. insoweit § 3 Abs. 8 Satz 3 BDSG). Sie werden gesetzlich einer internen Nutzung gleichgestellt und insoweit privilegiert.

Der Auftragnehmer ergreift unter anderem die folgenden Maßnahmen um zu gewährleisten, dass die Verarbeitung von Daten im Rahmen der Weisungen des Auftraggebers erfolgen kann.

Regelung der Auftragskontrolle.

a) Die Auftragnehmer werden unter besonderer Berücksichtigung der Eignung gemäß § 11 Abs. 2, Satz 1 ausgewählt ☐

b) Die Aufträge werden schriftlich erteilt gemäß § 11 Abs. 2, Satz 2 ☐

§ 11 Auftragsdatenverarbeitung - Abs. 2, Nr. 1 bis 10 (BDSG)

1. Der Gegenstand und die Dauer des Auftrags wird festgelegt ☐
2. Die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, der Kreis der Bertoffenen wird fixiert ☐
3. Der Nachweis zu § 9 plus Anlage wird eingeholt ☐
4. Die Berichtigung, Löschung und Sperrung von Daten werden fixiert ☐
5. Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen werden festgelegt ☐
6. Unterauftragsverhältnisse bedürfen der Zustimmung des Auftraggebers ☐
7. Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart ☐
8. Mitzuteilende Verstöße des Auftragnehmers sind vereinbart ☐
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält werden vereinbart ☐
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags werden vereinbart ☐

Auftragskontrolle

Allgemeine Beschreibung der Auftragskontrolle:

7. Verfügbarkeitskontrolle gemäß § 9 plus Anlage Nr. 7

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, z.B. durch Datensicherungen, Backups.

Regelung der Verfügbarkeitskontrolle.

- Unterbrechungsfreie Stromversorgung (USV) ☐
- Klimaanlage in Serverräumen ☐
- Überwachung von Temperatur und Feuchtigkeit in Serverräumen ☐
- Kabelverlegung nach DIN 18015 ☐
- Schutzsteckdosenleisten in Serverräumen ☐
- Feuer- und Rauchmeldeanlagen ☐
- Feuerlöschgeräte in Serverräumen ☐
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen ☐
- Erstellen eines Backup- und Recoverykonzeptes ☐
- Test von Wiederanlaufplänen ☐
- Erstellen eines Notfallplans ☐
- Aufbewahrung von Datensicherung an einem sicheren und ausgelagertem Ort ☐
- IT Brandnorm, Feuer - EN-1047-2 ☐
- Einbruchssicherheit, Fremdzugriff Norm - EN-1627 / EN-1630 ☐

Verfügbarkeitskontrolle

Allgemeine Beschreibung der Verfügbarkeitskontrolle:

8. Trennungsgebot gemäß § 9 plus Anlage Nr. 8

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

Regelung des Trennungsgebotes

- Daten werden ausschließlich zum Zweck der Erhebung verarbeitet ☐
- bei der Auftragsverarbeitung, erfolgt die Verarbeitung der Daten ausschließlich zum vereinbarten Zweck ☐
- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern ☐
- Berechtigungskonzept existiert ☐
- Trennung der Referenzdatei(Tabelle) bei pseudonymisierten Daten und der Aufbewahrung in einem abgesicherten IT-System ☐
- Trennung von Produktiv- und Testsystem ☐

_____, den _____

Ort Datum

_____

- Unterschriften Datenschutzbeauftragter und IT Leitung -