

**Technische und organisatorische Maßnahmen
zum Schutz personenbezogener Daten
gemäß § 9 und § 11 BDSG**

Unternehmen, „die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen“, haben die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten zu treffen (§ 9 BDSG). Im Falle einer Beauftragung gilt: „Werden personenbezogene Daten im Auftrag ... erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften ... verantwortlich. [...] Der Auftrag ist schriftlich zu erteilen, wobei die ... technischen und organisatorischen Maßnahmen festzulegen sind. [...] Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen“ (§ 11 BDSG).

Nachfolgend legt BusinessValues die erforderlichen Maßnahmen zur *innerbetrieblichen Organisation des Schutzes personenbezogener Daten* gemäß § 9 BDSG und der „Anlage zu § 9 Satz 1“ fest.

Diese Maßnahmen sind bei *Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag* gemäß § 11 BDSG durch auftragspezifische Weisungen des Auftraggebers in einem gesonderten Vertrag zu ergänzen.

1. Maßnahmen zur Zutrittskontrolle

Zu den Büroräumen von BusinessValues haben nur die Mitarbeiter von BusinessValues (nachfolgend Mitarbeiter genannt) Zutritt. Die Eingangstür ist mit einem Türschloss gesichert, zu dem nur die Mitarbeiter einen Schlüssel besitzen dürfen. Die Aus- und Rückgabe der Schlüssel ist zu dokumentieren. Durch Anwesenheitsaufzeichnungen ist zu dokumentieren, wann sich welcher Mitarbeiter in den Büroräumen aufgehalten hat. Betriebsfremde Personen dürfen nur im Büroraum auf der rechten Seite des Eingangsbereiches und nur unter Aufsicht eines Mitarbeiters empfangen werden.

2. Maßnahmen zur Zugangskontrolle

Zu den Datenverarbeitungsanlagen von BusinessValues haben nur die Mitarbeiter Zugang. Alle Datenverarbeitungssysteme von BusinessValues sind mit zweistufigen Zugangskennungen zu schützen. Sobald ein Mitarbeiter den Arbeitsplatz für länger als 10 Minuten verlässt und sich dafür nicht abmeldet, ist der Zugang automatisch zu sperren. Nutzerkennungen sind an den jeweiligen Nutzer gebunden und dürfen nicht an andere Personen weitergegeben werden.

3. Maßnahmen zur Zugriffskontrolle

Auf personenbezogene Daten von BusinessValues darf nur der Geschäftsführer zugreifen. Der Versuch, sich weitere, nicht vergebene Nutzerrechte zu erschleichen ist eine Straftat und zieht arbeits- wie strafrechtliche Konsequenzen nach sich.

4. Maßnahmen zur Weitergabekontrolle

Personenbezogene Daten dürfen nur über sichere Kommunikationswege übertragen werden. Der Versand per E-Mail ist nur in verschlüsselter Form zulässig.

Für die online an die gesetzlichen Krankenkassen zu übermittelnden Beitragsnachweise und Sozialversicherungsmeldungen ist das Programm *dakota* zu nutzen. *Dakota* dient der gesicherten Internet-Kommunikation und erfüllt entsprechende Auflagen der Datenschutzbeauftragten des Bundes und der Länder. Für die Datenübertragung liegt zudem ein Zertifikat durch das ITSG TrustCenter vor.

5. Maßnahmen zur Eingabekontrolle

Mit Hilfe personenbezogener Benutzerkonten muss nachvollziehbar sein, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind. Das kaufmännische Datenverarbeitungssystem *LexWare financial office plus* stellt entsprechende Datenbanktools zur Verfügung, die nur vom Geschäftsführer gestartet und genutzt werden dürfen.

Den Mitarbeitern von BusinessValues ist es untersagt, personenbezogene Daten mit Hilfe administrativer Benutzerkonten einzusehen oder zu verändern.

6. Maßnahmen zur Auftragskontrolle

Für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag gemäß § 11 BDSG gelten auftragsspezifische Weisungen des Auftraggebers. BusinessValues verpflichtet sich vorab,

- die im Auftrag zur Kenntnis gelangten personenbezogenen Daten strengstens geheim zu halten und nur insoweit zu verwenden, als dies für die Auftragsbearbeitung erforderlich ist
- diese Daten nicht zu veröffentlichen, mitzuteilen, zugänglich zu machen oder auf andere Weise zu verwerten
- diese Daten intern nur an solche Mitarbeiter von BusinessValues weiterzugeben, die mit der Auftragsbearbeitung betraut sind und die diese Daten für ihre Auftragsbearbeitung unbedingt benötigen
- die Einhaltung der Weisungen des Auftraggebers regelmäßig und gewissenhaft zu überwachen.

Alle darüber hinaus erforderlichen Maßnahmen zum Schutz der Datenerhebung, -verarbeitung, -nutzung oder -sicherung (vom Eingang der Daten bei BusinessValues bis zur Rückgabe an den Auftraggeber) sind in einem gesonderten schriftlichen Vertrag zwischen dem Auftraggeber und BusinessValues festzulegen.

7. Maßnahmen zur Verfügbarkeitsskontrolle

Personenbezogene Daten sind durch umfangreiche Datensicherungsmaßnahmen gegen zufällige Zerstörung oder Verlust zu schützen. Im Falle eines Verlustes muss eine Rekonstruktion der Daten möglich sein. Entsprechende Vorsorge ist vor allem durch ein verbindliches Datensicherungskonzept, ein leistungsfähiges Backup-Recovery-System, eine unterbrechungsfreie Stromversorgung sowie durch Schutz vor Brand- und Wasserschäden zu treffen.

Für die personenbezogenen Daten des kaufmännischen Datenverarbeitungssystems *LexWare financial office plus* ist darüber hinaus das Datenbanksicherungssystem von *LexWare* zu nutzen.

8. Trennungsgebot

Personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben werden (z.B. Test- oder Produktivdaten, eigene Daten oder im Auftrag erhobene Daten anderer Stellen) sind getrennt zu speichern und entsprechend ihrem Verarbeitungszweck getrennt zu verarbeiten. Dabei muss der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.

Geeignete Maßnahmen zur Trennung sind:

- Trennung der Datensätze durch Speicherung in logisch oder physikalisch getrennten Dateisystemen
- unterschiedliche Verschlüsselung von Datensätzen zur Abgrenzung der Zweckbindung
- Vergabe unterschiedlicher Zugriffsberechtigungen.