CLEVIS CONSULT

ZERTIFIKAT

Die Software

Personio der Personio GmbH

erfüllt alle geltenden Datenschutzvorschriften.

Geprüft wurden insbesondere:

- Möglichkeiten der gesicherten Authentisierung
- Rechte- und Rollenkonzept
- Technische und organisatorische Maßnahmen gem. § 9 BDSG

München, 18. Februar 2016

Holger Ringel
Geschäftsführer CLEVIS GmbH und
externer Datenschutzbeauftragter

CLEVIS GmbH
Erika-Mann-Str. 53
80636 München
Tel. +49 89 242 111-0
Fax +49 89 242 111-55
www.clevis-consult.de

Informationen zum Datenschutzzertifikat der Software *Personio*

Das Zertifikat für die Software *Personio* der *Personio GmbH* wurde nach Überprüfung folgender datenschutzrechtlicher Aspekte verliehen:

1. Zugangskontrolle
   a. Der Zugang zur Software ist durch zwingende Benutzerauthentisierung geschützt.
   b. Bei Daten mit höchstem Schutzniveau sind besonders hohe Anforderungen an die Authentisierung gestellt (Zwei-Faktor-Authentisierung).
   c. Bei Daten mit hohem Schutzniveau sind besondere Anforderungen an die Passwörter gestellt.
   d. Die Authentisierungsgeheimnisse werden nur verschlüsselt über das Netz übertragen.
   e. Nach Login-Fehlversuchen wird der Zugang gesperrt.
   f. Es existiert ein sicheres Verfahren zur Rücksetzung der Sperre.
   g. Ein Rollenkonzept mit vordefinierten Benutzerprofilen kann realisiert werden.
   h. Zugangsrechte können individuell und personengebunden vergeben werden.
   i. Alle erfolgreichen und abgewiesenen Zugangsversuche werden protokolliert und für mindestens sechs Monate revisionssicher archiviert.
   j. Tests zur Sicherstellung der Zugangskontrolle wurden implementiert.

2. Zugriffskontrolle
   a. Einzelne Berechtigungsprofile bzw. Benutzerrollen können angelegt, geändert und gelöscht werden.
   b. Jeder Zugriffsberechtigte kann nur auf die Daten zugreifen, die er zur Bearbeitung seiner aktuellen Aufgaben benötigt und die in dem individuellen Berechtigungsprofil eingerichtet sind.
   c. In der Software sind eindeutige Merkmale eingebaut, die es der zugreifenden Person ermöglichen, zu erkennen, dass es sich um eine authentische Software handelt.
   d. Der Umfang von Berechtigungen kann logisch und zeitlich auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung notwendige Minimum beschränkt werden.
   e. Berechtigungen sind immer an eine persönliche Benutzerkennung und an einen Account geknüpft.
   f. Entfällt die Grundlage für eine Berechtigung (z.B. durch eine Funktionsänderung) kann diese sofort entzogen werden.
   g. Alle Eingabe-, Änderungs- und Löschtransaktionen werden protokolliert (Benutzerkennung, Transaktionsdetails) und für mindestens sechs Monate revisionssicher archiviert.
   h. Tests zur Sicherstellung der Zugriffskontrolle wurden implementiert.

3. Verwendungszweckkontrolle
   a. Es gibt technische Möglichkeiten zur Sicherstellung der getrennten Verarbeitung und Lagerung von Daten.

4. Technische und organisatorische Maßnahmen des Softwareanbieters gem. § 9 BDSG
   a. Kundendaten werden auf Servern eines Drittanbieters gespeichert. Ein ADV-Vertrag liegt vor.
   b. Zwischen dem Softwareanbieter und seinen Kunden werden ADV-Verträge geschlossen.
   c. Der Softwareanbieter hat einen Datenschutzbeauftragten bestellt, der alle datenschutzrechtlichen Forderungen gem. § 9 BDSG kontrolliert.