Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO

der

Solvis GmbH

Grotrian-Steinweg-Straße 12

38112 Braunschweig

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Empfang mit Rezeption
- Besucherbuch und Protokollierung der Besucher
- Mitarbeiter- und Besucherausweise
- Besucher werden nur begleitet geführt
- Zutrittskontrollsystem mit persönlichem Mitarbeiterschlüssel
- Schlüsselausgabe wird dokumentiert, eine entsprechende Richtlinie ist vorhanden
- Separater Serverraum, ständig verschlossen. Zugang nur durch Leiter IT und dessen Vertreter

2. Zugangskontrolle

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

- Die Arbeitsplätze sind mit persönlichen, zeitlich begrenzten Kennwörtern gesichert. Jeder Mitarbeiter wird bei Einstellung informiert, dass bei Verlassen des Arbeitsplatzes die Arbeitsstation zu sperren ist. Zusätzlich sperrt eine Richtlinie den Arbeitsplatz automatisch nach 5 Minuten
- Benutzer werden entsprechend ihrem Aufgabenbereich in Gruppen mit Berechtigungen aufgenommen
- Es existiert eine Richtlinie für die Vergabe von starken Kennwörtern
- Mobile Geräte sind verschlüsselt und können remote zurückgesetzt werden
- Die Systeme werden zusätzlich mittels Anti-Viren Software geschützt
- W-LAN ist mit WPA2 gesichert

3. Zugriffskontrolle

Maßnahmen, die geeignet sind, zu 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.

- Es existiert für alle eingesetzten Systeme ein dediziertes Rechtesystem. Eine Zuteilung von Berechtigungen erfolgt erst nach Prüfung und Freigabe durch den Vorgesetzten. Die Berechtigungen werden regelmäßig überprüft
- Zugänge ausscheidender Mitarbeiter werden unmittelbar gesperrt
- Datenträger und Papierunterlagen werden durch professionellen Aktenvernichter zerstört

4. Weitergabekontrolle

Maßnahmen, die geeignet sind, 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 personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Mitarbeiterdaten sind getrennt von Kunden- und Projektdaten
- kein unbefugtes Lesen, Kopieren, verändern oder Entfernen bei elektronischer Übertragung oder Transport

5. Eingabekontrolle

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

- Versionsverwaltung von Dokumenten.
- Protokollierung der Zugriffe auf IT-Systeme
- Überwachung der Änderungen innerhalb der IT-Systeme

6. Auftragskontrolle

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

- Auswahl der AN erfolgt unter Berücksichtigung von Zertifizierungen bzw. Gütesiegeln
- Angaben der AN werden persönlich geprüft und dokumentiert

7. Verfügbarkeitskontrolle

Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Daten werden regelmäßig gesichert (Vollsicherung am Wochenende, unter der Woche täglich inkrementell. Monatssicherungen (extern) werden beim Systembereitsteller gelagert.
- Interne Sicherung auf NAS, HDD und Band in feuerfestem Safe
- Die Systeme werden an getrennten USVs betrieben und sind gegen Spannungsschwankungen abgesichert
- In den Serverräumen befinden sich unabhängige Klimaanlagen und Rauchmelder
- Alle Systeme befinden sich hinter einer Hardware-Firewall und sind ggf. durch weitere Software-Firewall zusätzlich geschützt
- Es kommt eine Antivirus-Lösung eines namhaften Herstellers zum Einsatz. Die Software wird ständig aktualisiert
- Ein Notfall- bzw. Wiederanlaufplan ist vorhanden

8. Trennungsgebot

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

- Personenbezogene Daten werden gesondert von Daten anderer Natur gesichert. Die Trennung ist durch ein Berechtigungskonzept mit Gruppen und Benutzern gewährleistet
- Der IT stehen, sofern notwendig, Testsysteme zur Verfügung bzw. werden kurzfristig eingerichtet. Der Einsatz von Testsystemen bei Kundenprojekten erfolgt in Kundenabsprache