

Im Rahmen der oben genannten Vereinbarung gibt die AG folgende konkret durch die AN sicherzustellenden technischen und organisatorischen Maßnahmen (Art. 28 Absatz 3 Satz 2 lit. c, Art. 32 DS-GVO) vor:

Maßnahmen bzgl. Räumlichkeiten & Gebäuden

- Allgemeine Vorgaben für alle Räumlichkeiten und Gebäude

- Die Eingänge zu allen Räumen und Gebäuden, in denen personenbezogene Daten verarbeitet werden, sind gegen den Zutritt Unbefugter hinreichend (z.B. Schlüssel, Token oder Karten [Zugangsmittel]) zu sichern. Unbefugten ist der Zugang zu verwehren.
- Die AN regelt die Zuständigkeit für die Ausgabe der Zugangsmittel schriftlich. Die Regelung enthält darüber hinaus auch Vorgaben zu Prüfintervallen hinsichtlich der Berechtigung an den Zugangsmitteln und dem Vorgehen beim Ausscheiden von Beschäftigten. Die Ausgabe und Rückgabe der Zugangsmittel sind zu protokollieren.
- Beschäftigte und Besucher sind auf Grund von schriftlichen Vorgaben der AN verpflichtet, Dienst- oder Besucherausweise jederzeit und gut sichtbar in den Räumlichkeiten und Gebäuden der AN zu tragen.
- Die AN stellt durch schriftliche Vorgaben und Kontrollen sicher, dass Fenster und Türen bei Verlassen des Raumes und außerhalb der Betriebszeiten der AN verschlossen sind.

- Zusätzliche Vorgaben für Serverräume und Rechenzentren

- Diese Räumlichkeiten sind gesondert gegen den Zutritt durch Unbefugte zu sichern. Die Sicherung ist so zu gestalten, dass das Betreten entgegen der Sicherung einen gesteigerten kriminellen Aufwand nötig machen würde.
- Der Eingangsbereich der Serverräume bzw. des Rechenzentrums ist durchgehend von einem Wachdienst besetzt, welcher sicherstellt, dass nur berechtigte Personen Zutritt erhalten. Alternativ ist auch eine elektronische Zugangskontrollanlage mit einer 2-Faktor-Authentifizierung zulässig. Das Betreten dieser Räumlichkeiten ist nur durch oder in Begleitung eines Beschäftigten der AN, des Wachdienstes oder SÜG überprüfte Personen zulässig. Der Zutritt zum Serverraum bzw. Rechenzentrum ist lückenlos zu protokollieren.
- In den eigentlichen Serverräumen gibt es keine Fenster und keine Leitungen usw. mit Flüssigkeiten über der Technik. Die Räumlichkeiten sind mit Gaslöschanlagen ausgestattet. Zumindest alle Außentüren sind videoüberwacht und alarmgesichert.
- Das Wach- und Reinigungspersonal ist sorgfältig auszuwählen (zumindest unter Vorlage eines Führungszeugnisses ohne einschlägige Eintragungen).
- Auf die Funktion der Räumlichkeiten bzw. des Gebäudes wird nicht zusätzlich z.B. durch Beschilderung hingewiesen.
- Gebäudeschächte sind gegen unberechtigtes Eindringen hinreichend abgesichert.
- Die wichtigsten Versorgungsleitungen sind redundant ausgelegt. Die AN stellt eine Notstromversorgung (z.B. USV-Anlagen usw.) von 3 Stunden sicher.
- In den Serverräumen gibt es Feuchtigkeits-, Rauch-, und Wärmesensoren deren Werte ständig überwacht werden.

- Die Mitnahme von Telefonen und Kameras in diese Räumlichkeiten ist nicht gestattet.

Maßnahmen bzgl. des Zugriffs auf personenbezogene Daten

- Die Zahl der zugriffsberechtigten Personen und insbesondere der Administratoren bei der AN wird durch sie auf das unvermeidbare Minimum begrenzt („need-to-know-Prinzip“). Dies erfolgt z.B. durch abgestufte Zugriffsrechte. Auch die Weitergabe der personenbezogenen Daten innerhalb des Unternehmens der AN ist auf ein absolutes Minimum zu begrenzen.
- Die AN stellt technisch sicher, dass die jeweilige Person ausschließlich auf diejenigen Daten Zugriff hat, auf die sich die Zugriffsberechtigung der Person erstreckt.
- Zu Wartungszwecken müssen gesonderte Zugriffsrechte bestehen, die einen Zugriff auf personenbezogene Daten soweit wie möglich ausschließen.
- Maßnahmen bzgl. Passwörtern
 - Die AN trifft schriftliche Regelungen zur Gestaltung und dem Umgang mit Passwörtern. Inhaltlich muss die Regelung zumindest vorgeben, dass die Passwörter mindestens eine Länge von 12 Zeichen aufweisen, jeweils Buchstaben, Zahlen und Sonderzeichen enthalten müssen und von den Beschäftigten geheim zuhalten sind. Weiter ist vorzugeben, dass Gruppenpasswörter nicht zulässig sind.
 - Die AN stellt technisch sicher, dass von den Systemen nur Passwörter akzeptiert werden, die den vorgenannten Vorgaben entsprechen und erzwingt spätestens alle 6 Monate technisch den Wechsel jedes Passworts. Weiter stellt die AN technisch sicher, dass die Passwörter zumindest innerhalb von zwei Jahren nicht erneut verwendet werden können.
 - Bei Arbeitsunterbrechungen ist technisch sicherzustellen, dass spätestens nach 5 Minuten ein passwortgeschützter Sperrbildschirm aktiviert wird.
 - Darüber hinaus gestaltet die AN die Arbeitsbereiche der Beschäftigten so, dass eine zufällige Kenntnisnahme der Passwörter durch Dritte bei der Eingabe durch den Berechtigten weitestgehend ausgeschlossen wird.

Weitere Maßnahmen

- Die AN hat alle Anmeldeversuche und Veränderungen zu protokollieren und technisch sicherzustellen, dass der Anmeldevorgang nach einer einstellbaren Anzahl von Fehlversuchen (max. 3) abgebrochen wird, vor einer Freigabe durch eine zentrale Stelle nicht erneut versucht werden kann und eine Benachrichtigung an eine zentrale Stelle bei der AN erfolgt, welche zur Aufklärung des Vorfalls zu verpflichten ist.
- Die AN verpflichtet sich auf allen Datenverarbeitungsanlagen Virens Scanner mit täglichen Updates und eine Firewall nach dem aktuellen Stand der Technik einzusetzen.
- Soweit personenbezogene Daten in Dokumenten (Papierform) oder Datenträgern vorliegen, sind diese sicher zu verschließen, wenn sie nicht gerade zur Erfüllung des Vertrages benötigt werden. Die vorgenannten Vorgaben sind durch schriftliche Vorgaben der AN sicherzustellen.
- Trennung von Produktiv- und Testumgebung
- Die AN hat dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.
- Soweit die AN neben denjenigen personenbezogenen Daten, die sie im Auftrag für die AG verarbeitet auch im Wege der Auftragsverarbeitung für andere AG tätig ist, muss eine zuverlässige Trennung/ Abschottung der Daten der verschiedenen AG durch die AN erfolgen.

Dies erfolgt im Idealfall durch eine physikalische Trennung der Daten. Gleiches gilt für die Daten – unabhängig ob personenbezogen oder nicht – der AN selbst.

- Die AN stellt (soweit dies in ihren Verantwortungsbereich fällt) sicher, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert oder verändert werden können.
- Die AN führt mindestens ein tägliches Backup der Daten (Totalsicherung) durch und stellt sicher, dass diese backup-Daten zumindest in einem anderen Brandabschnitt gespeichert werden.
- Bei der AN gibt es schriftliche Vorgaben zur Informationsweitergabe bei Störungen im Betrieb und bei Notfällen sowie Eskalationspläne.