Technisch Organisatorische Maßnahmen

Fronius International GmbH

Froniusstraße 1
4643 Pettenbach
Österreich

1. Zutrittskontrolle

1.1. Automatisches Zugangskontrollsystem

Beschreibung:

Der allgemeine Zutritt zu Gebäuden und zu den Räumlichkeiten erfolgt über ein elektronisches Zutrittskontrollsystem. Die Räumlichkeiten für die Mitarbeiter sind vom Kundenbereich getrennt und haben einen eigenen, elektronisch gesicherten Eingang. Damit wird gewährleistet, dass Besucher nicht unkontrolliert in den Mitarbeiterbereich gelangen können. Die Mitarbeiter sind nur soweit zutrittsberechtigt wie es für die Erfüllung ihrer täglichen Aufgaben notwendig ist.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Technische Maßnahme

1.2. Besucher nur in Begleitung

Beschreibung:

Besucher müssen sich am Empfang anmelden und können nur in Begleitung eines Fronius Mitarbeiters die Räumlichkeiten betreten.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Organisatorische Maßnahme

1.3. Chipkarten-/Transponder-Schließsystem

Beschreibung:

Der Zutritt zu schutzbedürftigen Teilen des Gebäudes ist mithilfe einer Zugangskontrolle abgesichert. Die Absicherung ist dabei mittels Chipkarten/Transpondern implementiert. Die Zutrittskontrolle steuert den Zutritt über ein festgelegtes Regelwerk, damit nur berechtigte Personen Zutritt zu den für sie freigegebenen Bereichen erhalten. Die Zutrittsberechtigungen können zeitlich begrenzt werden.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Technische Maßnahme

1.4. Einsatz eines Monitoring-Systems nach Stand der Technik

Beschreibung:

Die Auslastung der Server-Systeme und Netzwerkkomponenten wird laufend durch ein Monitoring-System nach dem Stand der Technik überwacht, um eine Überlastung frühzeitig zu erkennen und Systemparameter anzupassen.

Risiken:

Unzureichende Belastbarkeit der Systeme und Dienste, die im Zusammenhang mit der Verarbeitung stehen, gewährleisten.

1.5. Protokollierung von Besuchergruppen

Beschreibung:

Alle Besucher (in Gruppen) müssen sich mit Name, Firma, Zutritts- und Austrittszeit sowie Unterschrift schriftlich registrieren.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Organisatorische Maßnahme

1.6. Selbstverriegelnde Türen an der Außenseite

Beschreibung:

Türen an der Außenseite sind selbstverriegelnd ausgestattet. Beim Zutritt von Außen ist immer eine Zutrittskarte mit der entsprechenden Berechtigung oder ein entsprechender Schlüssel erforderlich.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Technische Maßnahme

1.7. Sorgfältige Auswahl bei Lieferanten und Partnern

Beschreibung:

Bei der Auswahl von externem Personal wie Wachdienst oder Reinigungspersonal wird besonderer Wert auf den guten Ruf und die Integrität des jeweiligen Dienstleisters gelegt. Bei Fremdpersonal ist es wichtig, dass die jeweilige Firma eine Verpflichtung zur Geheimhaltung und zur Wahrung des Datengeheimnisses unterfertigt und auch die Verpflichtung an die jeweiligen Mitarbeiter weitergibt. Bei kritischem Fremdpersonal wie Wachdienst ist der jeweilige Dienstleister dazu angehalten im Vorfeld ein Leumundszeugnis zur Prüfung der Unbedenklichkeit für die jeweilige Position vorzulegen.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Organisatorische Maßnahme

1.8. Videoüberwachung der Eingänge und Gebäude

Beschreibung:

Es wird ein Videoüberwachungssystem betrieben, um den Zutritt von unbefugten Personen zu überwachen und Straftaten (z. B. Einbruch) nachvollziehen zu können. Die Rahmenbedingungen des Datenschutzes werden beim Betrieb des Videoüberwachungssystems eingehalten. Die Videoüberwachung dient insbesondere auch dem Schutz von Daten.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Technische Maßnahme

2. Zugangskontrolle

2.1. Administrative Zugänge über Benutzerkonten

Beschreibung:

Administrative Zugänge zu Applikationen werden über dedizierte Benutzerkonten geschützt.

Risiken:

Nutzung von Unbefugten

Verhaltensregeln:

Technische Maßnahme

2.2. Authentifikation mit Benutzername / Passwort

Beschreibung:

Der Zugang zu allen IT-Systemen und Diensten ist durch Identifikation und Authentisierung mittels Benutzerkennung und Passwort abgesichert. Bei der Passwortvergabe müssen die Passwortrichtlinien (Maßnahme - Passwortrichtlinie) eingehalten werden.

Bei der Erstanmeldung der Benutzer werden Initialpasswörter verwendet, welche beim ersten Zugriff vom Benutzer geändert werden müssen. Die Passwörter dürfen nur dem jeweiligen Benutzer bekannt sein. Sollte das Passwort einer unautorisierten Person bekannt geworden sein, so muss das Passwort vom Benutzer sofort geändert werden.
Nach mehrfach aufeinanderfolgenden fehlerhaften Passworteingaben wird das jeweilige Benutzerkonto gesperrt.

Wird das Passwort vom Benutzer vergessen, muss beim Systemadministrator ein neues Passwort angefordert werden. Dieser hat dabei sicherzustellen, dass der anfordernde Benutzer auch wirklich derjenige ist, der er vorgibt zu sein.

Risiken:

Nutzung von Unbefugten

Verhaltensregeln:

Technische Maßnahme

2.3. Automatische Bildschirmsperre

Beschreibung:

Richtlinien zur Endgeräte-Compliance regeln die automatische Bildschirmsperre.

Es sind automatische Bildschirmsperre nach einer bestimmten Zeit eingerichtet, um automatisch nach Verlassen eines Arbeitsplatzes die Bildschirmsperre zu aktivieren. Die automatische Bildschirmsperre ist wichtig, wenn man den Arbeitsplatz verlässt und es versäumt manuell zu sperren. Dadurch wird der Einblick auf Daten durch unberechtigte Personen weitgehend verhindert.

Risiken:

Einsicht in Daten durch Unberechtigte

Verhaltensregeln:

Technische Maßnahme

2.4. Einsatz eines Firewall-Konzeptes

Beschreibung:

Das Fronius-Netzwerk wird durch ein Firewall-Konzept nach dem Stand der Technik geschützt.

Risiken:

Hacking, Zugriff von Unberechtigten, Diebstahl von Daten

Verhaltensregeln:

Technische Maßnahme

2.5. Einsatz von Anti-Viren-Software (Server, Client)

Beschreibung:

Zur Abwehr von Schadsoftware sind IT-Systeme mit einem aktuellen Anti-Malware-Lösung ausgestattet.

Dabei werden folgende grundlegende Anforderungen beachtet:

Die Virensignaturdateien müssen laufend automatisch aktualisiert werden.
Automatische Virensuchläufe über alle Datenträger des Computers müssen konfiguriert werden, um eine regelmäßige Prüfung des gesamten Datenbestandes zu
gewährleisten.
Der Virenscanner muss über einen aktiven Echtzeitschutz verfügen, um beim Zugriff auf eine Datei eine geeignete Warnung für den Benutzer ausgeben zu können.
Kann auf einem IT-System keine Anti-Viren-Software-Lösung installiert werden, sind geeignete anderweitige Maßnahmen (zB Application-Whitelisting) zu treffen.

Risiken:

Hacking, Trojaner, Viren, Ransomware

Verhaltensregeln:

Technische Maßnahme

2.6. Einsatz von geschütztem Wireless LAN (WLAN)

Beschreibung:

Das eingesetzte WLAN ist auf dem aktuellen Stand der Technik hinsichtlich der Security Implementierung. Bei der Positionierung der WLAN-Komponenten wurde darauf geachtet, dass diese vor unautorisiertem physischem Zugriff geschützt sind. Der Zugang zum Access-Point ist nicht über Standardpasswörter möglich. Das Passwort für einen Pre- Shared-Key muss gewisse Mindest-Anforderungen erfüllen. Es wird dafür Sorge getragen, dass die WLAN-Komponenten regelmäßige Firmware-/Software-Updates erhalten.

Gäste-WLAN: Das interne Firmennetzwerk darf für Besucher nicht zugänglich sein. Sollten Besucher Zugriff auf das Internet benötigen, wird ein separates Gäste-WLAN verwendet. Ein Zugriff auf das interne Firmennetzwerk darf über das Gäste-WLAN nicht möglich sein. Zugriffe auf das Gäste-WLAN wird nur über temporär gültige Zugangsdaten ermöglicht.

Risiken:

Hacking, Zugriff von Unberechtigten

Verhaltensregeln:

Technische Maßnahme

2.7. Einsatz von VPN-Technologie

Beschreibung:

Der Datenaustausch zwischen den Fronius-Standorten erfolgt grundsätzlich über dedizierter Leitungen oder über verschlüsselte VPN-Verbindungen. Ebenso erfolgt die VPN-Einwahl von Mitarbeitern über gesicherte Verbindungen. Bei VPN-Verbindungen ist eine Zweifaktor-Authentifizierung notwendig.

Die eingesetzte VPN-Lösung muss hinsichtlich Security dem aktuellen Stand der Technik entsprechen, die bedeutet:
* Verschlüsselte Verbindung gemäß dem Stand der Technik
* Authentifizierung der Client-Geräte mittels Zertifikat oder Zwei-Faktor-Authentifizierung

Risiken:

Nutzung von Unbefugten, Hacking

Verhaltensregeln:

Technische Maßnahme

2.8. Einsatz von zentraler Smartphone-Administrations-Software (Mobile Device Management)

Beschreibung:

Bei Smartphones kommt ein Mobile Device Management System (MDM) zum Einsatz, das die firmenbezogenen Daten in einem verschlüsselten Container vom Rest des Gerätes trennt.

Risiken:

Zugriff von Unberechtigten, Verlust und Diebstahl von Daten

Verhaltensregeln:

Technische Maßnahme

2.9. Erstellen von Benutzerprofilen

Beschreibung:

Es wird für jeden Benutzer ein Benutzerprofil erstellt. Es erfolgt eine Zuordnung von Benutzerprofilen zu IT-Systemen mit Zuordnung von speziellen Benutzerrechten. Für die Rücknahme von speziellen Benutzerrechten wird ebenfalls gesorgt.

Risiken:

Nutzung von Unbefugten

2.10. Festplattenverschlüsselung

Beschreibung:

Laptops werden bei Fronius durch Festplattenverschlüsselung entsprechend dem aktuellen Stand der Technik geschützt.

Risiken:

Zugriff von Unberechtigten, Diebstahl von Daten

Verhaltensregeln:

Technische Maßnahme

2.11. Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

Beschreibung:

Bei Fronius gibt es eine Passwort-Richtlinie, welche den richtigen Umgang mit Passwörtern definiert.

Risiken:

Zugriff von Unberechtigten

2.12. Regelmäßige Software Updates

Beschreibung:

Durch regelmäßige Updates werden meist Sicherheitslücken im Betriebssystem, beziehungsweise in einer Anwendung geschlossen.
Es werden daher, alle eingesetzten Anwendungen immer auf dem neusten Softwarestand gehalten. Updates lassen sich zentral verwalten und verteilen. Updates für Drittprogramme werden lokal auf den Geräten durchgeführt. Alle Geräte werden regelmäßig durch den Zuständigen (Asset-Owner) auf notwendige Updates überprüft, um sicherzustellen, dass alle Geräte auf dem neuesten Softwarestand sind.

Beim Beziehen der Updates wird darauf geachtet, diese nur direkt vom Softwarehersteller zu beziehen.
Bei Updates für betriebskritische Programme wird das Update zuerst auf einem Testsystem installiert und getestet, bevor es auf allen betroffenen Systemen installiert wird.

Risiken:

Zugriff von Unberechtigten, Hackerangriff, Verlust und Diebstahl von Daten

Verhaltensregeln:

Technische Maßnahme

2.13. Richtlinie Clean Desk

Beschreibung:

Mitarbeiter müssen bei Abwesenheit alle Informationsträger, welche personenbezogene Daten beinhalten, von ihrem Arbeitsplatz entfernen. Dadurch wird verhindert, dass unbefugte Personen Zugriff auf die Daten bekommen. Den Mitarbeitern werden dafür insbesondere verschließbare Schränke zur Verfügung gestellt. Beim Verlassen der Büroräumlichkeiten ist auf jeden Fall dafür Sorge zu tragen, dass alle Informationen ihrem Schutzbedarf entsprechend physisch versperrt werden oder der Raum so versperrt wird, dass unautorisierte Personen keinen Zutritt zum Raum erlangen können.

Risiken:

Zugriff von Unberechtigten

Verhaltensregeln:

Organisatorische Maßnahme

2.14. Richtlinie Clear Screen (manuelle Desktopsperre)

Beschreibung:

Computer oder andere Geräte mit Benutzer-Login sind bei jedem Verlassen des Arbeitsplatzes zu sperren (auch bei kurzen Pausen). Der Zuständige hat die Mitarbeiter über diese Maßnahme informiert und die Durchsetzung der Maßnahme wird regelmäßig geprüft.

Risiken:

Dateneinsicht durch Unberechtigte

Verhaltensregeln:

Organisatorische Maßnahme

2.15. Richtlinie Datenschutz und Informationssicherheit

Beschreibung:

Es wurde eine allgemein gültige Richtlinie zum Datenschutz und zur Informationssicherheit erstellt, die für alle Mitarbeiter verpflichtend einzuhalten ist. In dieser werden die Grundsätze und Rollen im Datenschutz, zur Informationsklassifizierung sowie diverse Verhaltensregeln festgelegt. Die Richtlinie wird periodisch überarbeitet und an den aktuellen Stand angepasst.

Risiken:

Datenschutzwidriges Verhalten, Dateneinsicht durch Unberechtigte

Verhaltensregeln:

Organisatorische Maßnahme

2.16. Richtlinie Mobile Geräte

Beschreibung:

Es wurde eine allgemein gültige Richtlinie für den Umgang mit mobilen Geräten erstellt. Darin werden Verhaltensregeln für die Sicherheit festgelegt. Diese Richtlinie ist allen Mitarbeitern bekannt und für diese auch verpflichtend einzuhalten.

Für Smartphones oder Geräte mit der Möglichkeit zu alternativen Authentisierungsverfahren gilt für die Gerätesperre:

* Verwendung eines PIN-Codes oder biometrisches Merkmal (zB Fingerabdruck oder Gesichtserkennung)
* Einfache Authentisierungsverfahren, wie zB Wischmuster sind unzulässig.

Risiken:

Datenschutzwidriges Verhalten, Dateneinsicht durch Unberechtigte

Verhaltensregeln:

Organisatorische Maßnahme

2.17. Richtlinie zur ordnungsgemäßen Vernichtung von Datenträgern / Löschung von Daten

Beschreibung:

Es wird sichergestellt, dass bei der Entsorgung von Informationsträgern ein angemessener Schutz gewährleistet wird, da ansonsten unbefugte Personen, beispielsweise beim Durchsuchen von Altpapiercontainern, unberechtigten Zugriff auf personenbezogene Daten erlangen könnten.

Es wurde ein Entsorgungskonzept erstellt, indem definiert wird, wie die Entsorgung von Datenträgern mit personenbezogenen Daten zu erfolgen hat. Papierdokumente müssen mittels Aktenvernichter oder über ein zertifiziertes Entsorgungsunternehmen vernichtet werden.

Elektronische Informationsträger müssen entweder sicher gelöscht oder physisch vernichtet werden (die physische Vernichtung elektronischer Informationsträger kann ebenfalls durch ein Entsorgungsunternehmen erfolgen). Geschieht die Entsorgung der Informationsträger über ein Entsorgungsunternehmen, so ist zu gewährleisten, dass die Informationsträger bis zur Abholung unter Verschluss gehalten werden.

Wichtig ist zu beachten, dass auch Kopierer meist eine Speichereinheit eingebaut haben, welche alle Kopiervorgänge speichert. Daher muss bei der Entsorgung eines Kopierers, diese Speichereinheit ausgebaut und wie andere elektronische Informationsträger sicher gelöscht oder physisch zerstört werden.

Alle Mitarbeiter werden vom Zuständigen über das Entsorgungskonzept informiert.

Risiken:

Zugriff von Unberechtigten

Verhaltensregeln:

Organisatorische Maßnahme

2.18. Umgang mit externen Wechseldatenträgern

Beschreibung:

Es existiert eine verpflichtende Regelung, dass Mitarbeiter keine Wechseldatenträger von betriebsfremden Personen an ihre Computer anschließen dürfen.

Sollte ein schneller Datenaustausch mit einer betriebsfremden Person unbedingt notwendig sein, sollten die Daten via E-Mail ausgetauscht und die empfangenen Daten mittels Virenscanner geprüft werden, bevor diese weiterverwendet werden. Auch der Austausch via explizit freigegebener Datenaustauschplattformen ist möglich.

Risiken:

Nutzung von Unbefugten, Trojaner, Ransomware

Verhaltensregeln:

Organisatorische Maßnahme

2.19. Verschlüsselung von Laptops / Notebooks

Beschreibung:

Notebooks / Tablets werden verschlüsselt um im Falle des Verlustes oder Diebstahls darauf befindliche Daten vor unberechtigtem Zugriff zu schützen. Hierbei werden kryptografische Verfahrens nach Stand der Technik verwendet.

Risiken:

Zugriff von Unberechtigten, Verlust und Diebstahl von Daten

Verhaltensregeln:

Technische Maßnahme

2.20. Verschlüsselung von mobilen Datenträgern

Beschreibung:

Mobile Geräte und externe Datenträger (USB-Stick, USB-Festplatte), auf denen personenbezogene Daten gespeichert werden, sind zu verschlüsseln. Dadurch kann bei einem Verlust oder Diebstahl des Geräts verhindert werden, dass unbefugte Personen Zugriff auf die gespeicherten Daten erhalten. Bei der Vergabe des Verschlüsselungspasswortes gilt die Passwortrichtlinie aus Maßnahme.

Risiken:

Nutzung von Unbefugten bei Verlust

Verhaltensregeln:

Technische Maßnahme

2.21. Verschlüsselung von Smartphone-Inhalten

Beschreibung:

Auf Smarthpones werden ausschließlich dem autorisierten Nutzer Zugriff auf Daten gewährt. Es wird durch Verschlüsselung des gesamten mobilen Systems verhindert, dass ohne den passenden Zugangsschlüssel, die Daten von unberechtigten Dritten ausgelesen werden können. Dies bietet einen zusätzlichen Schutz, falls ein Gerät verloren oder gestohlen wurde.

Risiken:

Nutzung von Unbefugten bei Verlust

Verhaltensregeln:

Technische Maßnahme

2.22. Verwaltung von Benutzerberechtigungen

Beschreibung:

Die Einrichtung von Benutzern und Berechtigungsgruppen geschieht durch den jeweils dafür Zuständigen. Dieser teilt den Benutzern Berechtigungen auf Ressourcen zu, beziehungsweise entzieht diese. Außer dem Zuständigen darf niemand administrativen Zugang auf ein IT-System haben.

Risiken:

Nutzung von Unbefugten

Verhaltensregeln:

Organisatorische Maßnahme

2.23. Zentrale Passwortvergabe

Beschreibung:

Die IT-Systeme verfügen über ein Berechtigungskonzept mittels Passwortzugang. Es wird vom System vorgegeben, dass nur Passwörter mit einer gewissen Mindestlänge verwendet werden können. Dort wo es sinnvoll ist, wird ein regelmäßiges Ändern der Passwörter erzwungen.

Risiken:

Nutzung von Unbefugten

3. Zugriffskontrolle

3.1. Anzahl der Administratoren auf das „Notwendigste“ reduziert

Beschreibung:

Die Anzahl der Systemadministratoren ist auf die minimal notwendige Anzahl an Personen reduziert.
Es wird sichergestellt, dass nur ausgewählte Personen mit dem notwendigen technischen Know-How als Systemadministratoren benannt werden. Bei der Anzahl der Systemadministratoren wird stets die Anzahl der Mitarbeiter und die Anzahl der Spezialsoftware und Server beachtet.

Risiken:

Datenzugriff von Unbefugten

Verhaltensregeln:

Organisatorische Maßnahme

3.2. Einsatz eines Berechtigungskonzepts

Beschreibung:

Bei Applikationen, bei denen personenbezogene Daten verarbeitet werden, kommt ein rollenbasiertes Berechtigungskonzept zum Tragen. Berechtigungen werden nur nach Freigabe der jeweiligen Fachbereichsverantwortlichen vergeben und nur diejenigen Mitarbeiter erhalten Zugriff, für deren Arbeit der Zugriff notwendig ist (Least-Priviledge-Prinzip).

Die vergebenen Berechtigungen werden zumindest jährlich auf Notwendigkeit überprüft und entzogen, wenn der Benutzer diese nicht mehr zur Erfüllung seiner Aufgaben benötigt.

Sollte ein Mitarbeiter die Abteilung oder das Aufgabengebiet wechseln, so sind seine Berechtigungen erneut zu prüfen und gegebenenfalls zu berichtigen. Berechtigungen, welche nicht mehr benötigt werden, sind umgehend zu entfernen. Bei einem Austritt des Mitarbeiters sind diesem alle vergebenen Berechtigungen zu entziehen.
Sollte eine Berechtigung zwischen mehreren Mitarbeitern geteilt worden sein (zB: Gruppenbenutzer mit gemeinsamem Passwort), so ist das Passwort nach Ausscheiden eines Mitarbeiters sofort zu ändern.

Risiken:

Datenzugriff von Unbefugten

Verhaltensregeln:

Organisatorische Maßnahme

3.3. Einsatz von externen Aktenvernichtern bzw. Dienstleistern

Beschreibung:

Für die Entsorgung von großen Dokumentenmengen sowie von Festplatten werden im Bedarfsfall zertifizierte Dienstleister mit der Vernichtung beauftragt. Ansonsten werden Aktenschredder verwendet.

Risiken:

Unbefugte Veröffentlichung, Zugriff von Unberechtigten, Datenverlust

Verhaltensregeln:

Organisatorische Maßnahme

3.4. physische Löschung von Datenträgern vor Wiederverwendung

Beschreibung:

Vor Wiederverwendung eines Datenträger wird durch geeignete (physikalische) Maßnahmen oder durch mehrmaliges Überschreiben von Daten gewährleistet, dass die Daten sicher, dh. vollständig und unumkehrbar gelöscht werden.

Risiken:

Datenzugriff und Dateneinsicht von Unbefugten

Verhaltensregeln:

Technische Maßnahme

3.5. Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

Beschreibung:

In den verschiedenen Systemen werden Änderungen an Stammdaten protokolliert. Nicht alle Eingabefelder werden automatisch protokolliert. Rechte zur Änderung von Daten sind an die jeweilige Benutzerrolle gebunden.

Risiken:

Datendiebstahl, Zugriff von Unberechtigten, Datenverlust

Verhaltensregeln:

Technische Maßnahme

3.6. Sichere Aufbewahrung von Datenträgern

Beschreibung:

Informationsträger mit personenbezogenen Daten dürfen nicht öffentlich zugänglich sein und sind somit wegzusperren, sobald kein Mitarbeiter mehr vor Ort ist. Sollte es nicht möglich sein, die Informationsträger an öffentlich zugänglichen Orten zu verschließen, so sind diese zu verschlüsseln.
Externe Datenträger (USB-Sticks, externe Festplatten) werden verschlüsselt.

Risiken:

Datenzugriff von Unbefugten

Verhaltensregeln:

Organisatorische Maßnahme

3.7. Verwaltung der IT-Infrastruktur durch ausgebildete Systemadministratoren

Beschreibung:

Die Verwaltung, Überwachung und Weiterentwicklung der Netzwerke und IT-Strukturen wird durch eigene Systemadministratoren verantwortet. Für die Position des Systemadministrator werden tiefgreifende Computer- und Netzwerkkenntnisse verlangt, ebenso wie die Eigenschaft zur schnellen Problemlösung.

Risiken:

Datenzugriff von Unbefugten

Verhaltensregeln:

Organisatorische Maßnahme

3.8. Verwendung eines Datenschutztresors

Beschreibung:

Um Speichermedien wie Festplatten und andere Datenträger (insbesondere Sicherungsbänder) sicher aufzubewahren wird ein zertifizierter und genormter Datenschutztresor verwendet. Der Datenschutztresor bietet dabei Diebstahlschutz und Schutz vor Datenverlust bei einem Brand.

Risiken:

Datendiebstahl, Zugriff von Unberechtigten, Datenverlust

Verhaltensregeln:

Organisatorische Maßnahme

3.9. Verwendung von datenschutzkonformen Aktenschreddern für Daten mit erhöhtem Schutzbedarf

Beschreibung:

Bei der Aktenvernichtung von besonders schutzwürdigen personenbezogenen Daten werden Aktenvernichter mit mindestens Schutzklasse 3 und cross-cut eingesetzt. Damit wird eine unbefugte Öffentlichwerdung der betroffenen Informationen verhindert.

Risiken:

Unbefugte Veröffentlichung, Zugriff von Unberechtigten, Datenverlust

Verhaltensregeln:

Technische Maßnahme

4. Weitergabekontrolle

4.1. Bereitstellung von Daten über verschlüsselte Verbindungen

Beschreibung:

Sofern Daten auf elektronischem Weg ausgetauscht werden müssen, erfolgt die Übertragung ausschließlich über eine sichere und verschlüsselte Datenverbindung.

Risiken:

Zugriff von Unberechtigten

Verhaltensregeln:

Technische Maßnahme

4.2. Dokumentation der Empfänger von Daten

Beschreibung:

Bei Datenübermittlungen wird der Empfänger von Daten bei den jeweiligen Datenverarbeitungen dokumentiert. Dies ermöglicht die rechtskonforme Beantwortung von Auskunftsanfragen und die Nachverfolgung von Übermittlungsvorgängen.

Risiken:

Zugriff von Unberechtigten, rechtsgrundlose Verarbeitung von Daten

Verhaltensregeln:

Organisatorische Maßnahme

4.3. Nutzung von Signaturverfahren

Beschreibung:

Beim Datenaustausch kommt bei der Authentifizierung ein sicheres Signaturverfahren zur Anwendung. Das Signaturverfahren basiert dabei auf einem asymetrischen Verfahren und entspricht dem Stand der Technik.

Risiken:

Zugriff von Unberechtigten

Verhaltensregeln:

Technische Maßnahme

4.4. Weitergabe von Daten in pseudonymisierter Form

Beschreibung:

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

Risiken:

Datenverlust, Dateneinsicht durch Unberechtigte

Verhaltensregeln:

Organisatorische Maßnahme

5. Eingabekontrolle

5.1. Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

Beschreibung:

Bei der Übernahme von Daten aus Formularen, werden auch die Formulare noch eine gewisse Zeit aufbewahrt um mögliche Fehler in der Dateneingabe nachvollziehen zu können.

Risiken:

Verfälschung von Daten, Datenverlust, fehlende Datenintegrität

Verhaltensregeln:

Organisatorische Maßnahme

5.2. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Beschreibung:

Aufgrund Art 5 DSGVO ist es notwendig, nachvollziehen zu können, zu welcher Zeit und von welchem Benutzer personenbezogene Daten eingefügt, geändert oder gelöscht wurden. Es wurde daher bei Applikationen je nach Möglichkeit eine Protokollierung für die Nachvollziehbarkeit von Eingaben implementiert. Gruppenzugänge sind nicht zugelassen.

Risiken:

Verfälschung von Daten, Datenverlust, Zugriff von Unberechtigten, rechtsgrundlose Verarbeitung von Daten

Verhaltensregeln:

Organisatorische Maßnahme

5.3. Technische Protokollierung der Eingabe, Änderung und Löschung von Daten

Beschreibung:

In den verschiedenen Systemen werden Änderungen an Stammdaten protokolliert. Nicht alle Eingabefelder werden automatisch protokolliert. Rechte zur Änderung von Daten sind an die jeweilige Benutzerrolle gebunden.

Risiken:

Verfälschung von Daten, Zugriff von Unberechtigten, rechtsgrundlose Verarbeitung von Daten

Verhaltensregeln:

Technische Maßnahme

6. Auftragskontrolle

6.1. Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln

Beschreibung:

Auftragsverarbeiter Verträge sind verpflichtend abzuschließen. Bei Auftragsverarbeitungen außerhalb des EWR und außerhalb eines sicheren Drittlandes kommen die EU-Standardvertragsklauseln für die Datenverarbeitung zur Anwendung. Darüber hinaus vereinbart Fronius als Verantwortliche mit den Auftragsverarbeitern für den Fall von Datenübermittlungen außerhalb der EU/EWR soweit wie möglich weitere vertragliche, technische und organisatorische Maßnahmen und Regelungen bzw. Zusicherungen, um ein der DSGVO entsprechendes Datenschutzniveau sicherzustellen.

Risiken:

unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

6.2. Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Informationssicherheit)

Beschreibung:

Bei der Auswahl von Auftragnehmern die mit der Verarbeitung personenbezogener Daten betraut sind, ist höchstes Augenmerk auf die Themen Datenschutz und Informationssicherheit zu legen. Es ist durch geeignete Vorkehrungen sichergestellt, dass im Auswahlprozess diese Themen vorrangig beachtet werden und eine maßgebliche Entscheidungsgrundlage für die Beauftragung sind.

Risiken:

Mißbräuchliche Verwendung der Personendaten, unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

6.3. Dokumentierte Weisungen an den Auftragnehmer

Beschreibung:

Es ist sichergestellt, dass mit jedem Auftragnehmer der mit der Verarbeitung personenbezogener Daten betraut wird eine Vereinbarung zur Auftragsverarbeitung getroffen wird. Weisungen an den Auftragnehmer sind stets dokumentiert zu verfassen und auch bereits Inhalt einer Standard-Auftragsverarbeitervereinbarung. Die Weisungen können auch bereits aus dem Hauptvertrag bzw. aus der konkreten Leistungsvereinbarung hervorgehen. Für diesen Fall wird im Auftragsverarbeitungsvertrag darauf verwiesen.

Risiken:

Mißbräuchliche Verwendung der Personendaten, unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

6.4. Regelung zum Einsatz weiterer Sub-Unternehmer

Beschreibung:

Im Auftragsverarbeitungsvertrag ist für die Beauftragung weiterer Sub-Unternehmer festgelegt, dass ohne Information und Einspruchsrecht eine Subvergabe durch den Auftragnehmer nicht erfolgen kann. Darüber hinaus wird dem Auftragsverarbeiter die Verantwortung für die Einhaltung des Auftragsverarbeitungsvertrags durch einen Subauftragsverarbeiter auferlegt sowie der Auftragsverarbeiter nach Möglichkeit verpflichtet, für den Fall von Datenübermittlungen außerhalb der EU/EWR entsprechende weitere vertragliche, technische und organisatorische Garantien mit seinen Subauftragsverarbeitern zu vereinbaren, um ein der DSGVO entsprechendes Datenschutzniveau sicherzustellen.

Risiken:

unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

6.5. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Beschreibung:

Im Auftragsverarbeitungsvertrag ist die Verpflichtung festgehalten, dass der Auftragnehmer nach Beendigung des Auftragsverhältnisses die Daten unverzüglich an den Auftraggeber zurückzustellen oder nach Entscheidung durch den Auftraggeber zu vernichten hat.

Risiken:

Mißbräuchliche Verwendung der Personendaten, unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

6.6. Verpflichtung der eigenen Mitarbeiter sowie der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Beschreibung:

Alle Mitarbeiter der Fronius International GmbH unterschreiben mit ihrem Dienstvertag einen Passus, welcher sie zur Vertraulichkeit bei der Verarbeitung von personenbezogenen Daten verpflichtet. Bei der Zusammenarbeit mit anderen Unternehmen oder Organisationen werden Vertraulichkeitsvereinbarungen (NDAs) unterzeichnet. In Auftragsverarbeitungsverträgen wird der Auftragsverarbeiter dazu verspflichtet, auch seine Mitarbeiter zum Datengeheimnis und zur Vertraulichkeit zu verpflichten.

Risiken:

Mißbräuchliche Verwendung der Personendaten, unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

6.7. Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Beschreibung:

Im Auftragsverarbeitungsvertrag ist die Verpflichtung festgehalten, dass der Auftragnehmer Mitarbeitern nur nach unbedingter Notwendigkeit Daten zur Kenntnis bringen darf. Jeder Mitarbeiter des Auftragnehmers ist ausnahmslos auf das Datengeheimnis im gesetzlichen Umfang zu verpflichten.

Risiken:

Mißbräuchliche Verwendung der Personendaten, unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

6.8. Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen einer Bestellpflicht

Beschreibung:

In Auftragsverarbeitungsverträgen wird vereinbart, dass der Auftragnehmer die gesetzliche Voraussetzung zur Bestellung eines Datenschutzbeauftragten gem. Art 38f DSGVO zu prüfen hat. Im Falle der gesetzlichen Notwendigkeit ist es unbedingt erforderlich und auch per vertraglicher Verpflichtung festgehalten, dass der Auftragnehmer einen Datenschutzbeauftragten bestellt.

Risiken:

Mißbräuchliche Verwendung der Personendaten, unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

6.9. vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

Beschreibung:

Im Zuge der Auswahl von Dienstleister wird deren dokumentierte Sicherheitsmaßnahmen eingefordert und stichprobenweise überprüft. Soweit es die Möglichkeit gibt, können in Einzelfällen auch Vor-Ort-Prüfungen durchgeführt werden. Die dokumentierten Sicherheitsmaßnahmen müssen jeweils dem Stand der Technik entsprechen und angepasst werden und können periodisch eingefordert werden.

Risiken:

Mißbräuchliche Verwendung der Personendaten, unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

6.10. Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

Beschreibung:

Im Auftragsverarbeitungsvertrag sind wirksame Kontrollrechte gegenüber dem Auftragnehmer festgelegt. Im Falle des Zuwiderhandelns wäre der Auftragnehmer vertragsbrüchig. Es kann jederzeit, ohne Störung des Betriebes des Auftragnehmers, eine Vor-Ort-Kontrolle durchgeführt werden.

Risiken:

Mißbräuchliche Verwendung der Personendaten, unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

7. Verfügbarkeitskontrolle

7.1. Alarmmeldung bei unberechtigten Zutritten zu Serverräumen

Beschreibung:

Der Zutritt zum Serverraum wird durch eine Alarmanlage überwacht. Jeder unberechtigte Zutritt löst dabei eine Alarmmeldung aus auf die unverzüglich reagiert werden kann.

Risiken:

Datendiebstahl, Zugriff von Unberechtigten

Verhaltensregeln:

Technische Maßnahme

7.2. Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Beschreibung:

Sicherungen von Daten werden an einem getrennten Standort der Live-Daten aufbewahrt.

Risiken:

Datenverlust

Verhaltensregeln:

Organisatorische Maßnahme

7.3. Brandfrüherkennungsanlagen

Beschreibung:

Brandfrüherkennungsanlagen dienen der schnellen Branderkennung insbesondere der vorausschauenden Brandvermeidung.

Risiken:

Datenverlust

Verhaltensregeln:

Technische Maßnahme

7.4. Existenz eines Notfallplans

Beschreibung:

Es wurden mögliche Risiken in den IT-Systemen identifiziert und ein Notfallplan erstellt. Darin werden Handlungsoptionen für den Ernstfall aufgeführt. Die notwendigen Schritte zur Wiederherstellung der Daten sind in einem Datensicherungskonzept dokumentiert, damit die Daten im Bedarfsfall auch durch fachkundige Dritte wiederhergestellt werden können. Der Notfallplan ist den IT-Mitarbeitern bekannt. Gleichzeitig wird der Notfallplan auch an gesicherter dritter Stelle aufbewahrt.

Risiken:

Datenverlust

Verhaltensregeln:

Organisatorische Maßnahme

7.5. Feuerlöschgeräte in Serverräumen

Beschreibung:

Im Serverraum ist ein Handfeuerlöscher vorhanden.

Risiken:

Datenverlust

Verhaltensregeln:

Technische Maßnahme

7.6. Firewall-Konzept und Penetrationtests

Beschreibung:

Das Fronius-Netzwerk wird durch ein Firewall-Konzept nach dem Stand der Technik geschützt. Für extern erreichbare Systeme werden Penetrationtests durchgeführt und dokumentiert.

Risiken:

zufällige oder mutwillige Zerstörung bzw. Verlust der Daten

7.7. Fronius Backupkonzept und Sicherheitsupdates

Beschreibung:

Die Daten werden auf Speichersystemen nach dem Stand der Technik gespeichert. Des Weiteren werden die Daten regelmäßig gesichert und die Sicherungen ausgelagert.
Verfügbare Sicherheitsupdates werden bei Server und Clients installiert. Die Ausrollung dieser Updates wird über entsprechende Reports überprüft.

Außerdem sind die Mitarbeiter verpflichtet, alle dienstlichen Daten ausschließlich auf den vom Datensicherungskonzept umfassten, gesicherten Laufwerken/ Servern zu speichern.

Risiken:

Datenverlust, fehlende Datenintegrität, zufällige oder mutwillige Zerstörung bzw. Verlust der Daten

Verhaltensregeln:

Organisatorische Maßnahme

7.8. Geräte zur Überwachung von Temperatur in Serverräumen

Beschreibung:

Bei etwaigen Abweichungen der Betriebsparameter wird ein entsprechender Alarm ausgelöst. Um Hitze- und / oder Feuchtigkeitsentwicklungen im Serverraum vorzubeugen werden zur Überwachung von Temperatur und Feuchtigkeit spezielle Geräte verwendet. Bei Alarm durch diese Geräte kann kurzfristig reagiert und dadurch Gefahren abwendet werden.

Risiken:

Datenverlust

Verhaltensregeln:

Technische Maßnahme

7.9. Klimaanlage in Serverräumen

Beschreibung:

Die Fronius-Datacenter sind klimatisiert, mit einer unterbrechungsfreien Stromversorgung ausgestattet und werden laufend überwacht.

Risiken:

Datenverlust

Verhaltensregeln:

Technische Maßnahme

7.10. Mehrstufiges Anti-Malware-Sicherheitskonzept nach Stand der Technik

Beschreibung:

Zum Schutz vor Schadsoftware findet ein mehrstufiges Anti-Malware-Sicherheitskonzept nach dem Stand der Technik Anwendung.

Risiken:

zufällige oder mutwillige Zerstörung bzw. Verlust der Daten

7.11. Redundante Auslegung von IT-Systemen

Beschreibung:

IT-Systeme sind bei Bedarf redundant ausgelegt. Daten werden im laufenden Betrieb mit vollständiger Redundanz gleichzeitig auf mehreren Festplatten gespeichert. Dadurch sind die Daten auch bei Ausfall eines Laufwerks immer noch auf einem anderen Laufwerk vorhanden. Die Festplattenspiegelung ist eine weitere Maßnahme zur Datensicherheit.

Risiken:

zufällige oder mutwillige Zerstörung bzw. Verlust der Daten

7.12. Regelmäßige Tests zur Datenwiederherstellung

Beschreibung:

Die Wiederherstellung von Backups wird regelmäßig überprüft und dokumentiert.

Risiken:

Datenverlust

Verhaltensregeln:

Organisatorische Maßnahme

7.13. Schutz vor DoS-Angriffen

Beschreibung:

Die Fronius Systeme sind durch unterschiedliche Schutzsysteme vor DoS-Angriffen abgesichert

Risiken:

Unzureichende Belastbarkeit der Systeme und Dienste, die im Zusammenhang mit der Verarbeitung stehen, gewährleisten

7.14. Speicherung in Versionskontrollsystemen

Beschreibung:

Zur Nachvollziehbarkeit von Änderungen werden wichtige Daten in Versionskontrollsystemen gespeichert.

Risiken:

zufällige oder mutwillige Zerstörung bzw. Verlust der Daten

7.15. Überspannungsschutz in Serverräumen

Beschreibung:

Zum Schutz von Überspannungsschäden werden USVs (ununterbrechbare Stromversorgung) mit Spannungsfilter eingesetzt.

Risiken:

Datenverlust

Verhaltensregeln:

Technische Maßnahme

7.16. Unterbrechungsfreie Stromversorgung (USV) und Notstromaggregate

Beschreibung:

Es wird eine unterbrechungsfreie Stromversorgung eingesetzt, um bei Störungen im Stromnetz die Versorgung kritischer IT-Systeme sicherzustellen. Empfindliche Geräte werden dadurch in ihrer Funktion weder beeinträchtigt noch beschädigt. Die USV gleicht dabei lokale Schwankungen und Ausfälle aus, indem angeschlossene Geräte mit elektrischer Energie aus Akkumulatoren gespeist werden, welche ständig aus dem Stromnetz nachgeladen werden. Darüber hinaus können längerfristige Ausfälle durch ein mit Kraftstoff betriebenes Notstrom-Aggregat überbrückt werden.

Risiken:

Datenverlust

Verhaltensregeln:

Technische Maßnahme

7.17. Verwendung eines Datenschutztresors

Beschreibung:

Um wichtige Daten vor Zerstörung, Verlust oder Schädigung zu schützen kommt zur sicheren Aufbewahrung ein Datenschutztresor zum Einsatz. Es wurde bei der Anschaffung des Datenschutztresors auf Zertifizierungen zum Datenschutz und zur Datensicherheit sowie insbesondere auf die notwendige Hitzebeständigkeit geachtet.

Risiken:

Datenverlust, Datenschädigung, Datenzerstörung

Verhaltensregeln:

Technische Maßnahme

7.18. Videoüberwachung Serverraum

Beschreibung:

Die Datacenter sind mit einem Videoüberwachungssystem ausgestattet.

Risiken:

Datendiebstahl, Zugriff von Unberechtigten

Verhaltensregeln:

Technische Maßnahme

7.19. Zugangskontrolle zu Serverräumen inklusive Alarmsicherung

Beschreibung:

Die Fronius-Rechenzentren sind stark zugangsbeschränkt. Zusätzlich zur elektronischen Zutrittskontrolle dient eine Alarmsicherung und Weiterleitung als zweiter Authentifizierungsfaktor. Nur wenige, geschulte Mitarbeiter haben Zutritt zu den Fronius-Datacentern. Deren Zutrittsfreigabe erfolgt erst nach Einschulung und schriftlicher Freigabe der Führungskräfte zweier definierter Fachbereiche. Sollten dritte Personen Zugang zum Rechenzentrum benötigen, werden Sie von einem autorisierten Fronius-Mitarbeiter begleitet und während des gesamten Aufenthalts beaufsichtigt. Zutritte über das Zutrittskontrollsystem werden zentral protokolliert.

Risiken:

Datendiebstahl, Zugriff von Unberechtigten

Verhaltensregeln:

Technische und organisatorische Maßnahme

8. Trennungsgebot

8.1. Festlegung von Datenbankrechten

Beschreibung:

Für den Zugriff auf Datenbanken gibt es ein spezielles Berechtigungskonzept. Die Berechtigungen werden nur im notwendigen Umfang vergeben. Rechte werden auch wieder entzogen, falls kein Zugriff mehr notwendig ist.

Risiken:

Datenverlust, Datenpanne, unberechtigter Zugriff

Verhaltensregeln:

Organisatorische Maßnahme

8.2. Mandantenfähigkeit relevanter Anwendungen

Beschreibung:

Je höher der Schutzbedarf und das Risiko für personenbezogene Daten ist, desto höher sind die Ansprüche an Mandantentrennung. Daher wird darauf geachtet, dass relevante Datenanwendungen jedenfalls mandantenfähig sind. Es wird damit sichergestellt, dass mehrere Nutzer Anwendungen gleichzeitig verwenden können, ohne die Daten der anderen User einsehen zu können.

Risiken:

Datenverlust, Datenpanne, Zugriff von Unberechtigten, Diebstahl von Daten

Verhaltensregeln:

Technische Maßnahme

8.3. Rollenbasiertes Berechtigungskonzept

Beschreibung:

Bei Applikationen, bei denen personenbezogene Daten verarbeitet werden, kommt ein rollenbasiertes Berechtigungskonzept zum Tragen.

Risiken:

Zu unterschiedlichen Zwecken erhobene personenbezogene Daten können nicht getrennt verarbeitet werden

Verhaltensregeln:

Berechtigungen werden nur nach Freigabe der jeweiligen Fachbereichsverantwortlichen vergeben und nur diejenigen Mitarbeiter erhalten Zugriff, für deren Arbeit der Zugriff notwendig ist.

8.4. Steuerung der Datentrennung über ein Berechtigungskonzept

Beschreibung:

Eine Trennung der Daten zu unterschiedlichen Zwecken erfolgt über ein Berechtigungskonzept, welches den Zugriff auf personenbezogene Daten regelt. Die Datentrennung erfolgt dabei virtuell. Es ist sichergestellt, dass Nutzer nur die unbedingt erforderlichen Berechtigungen erhalten und diese nach Wegfall der Erforderlichkeit auch wieder entzogen werden.

Risiken:

Datenverlust, Datenpanne, Zugriff von Unberechtigten, Diebstahl von Daten

Verhaltensregeln:

Organisatorische Maßnahme

8.5. Trennung von Produktiv- und Testsystem

Beschreibung:

Test- und Produktivsystem werden immer auf unterschiedlichen Servern betrieben.

Risiken:

Datenverlust, Datenpanne

Verhaltensregeln:

Technische Maßnahme

8.6. Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

Beschreibung:

Sofern für die jeweilige Datenverarbeitung möglich, werden Verschlüsselungstechnologien nach dem Stand der Technik eingesetzt.

Risiken:

Datenverlust, Datenpanne, fehlende Zweckbindung, unrechtmäßige Verarbeitung von Daten, unberechtigter Zugang

Verhaltensregeln:

Technische Maßnahme

9. Pseudonymisation

9.1. Pseudonymisierung von Daten

Beschreibung:

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

Risiken:

Dateneinsicht durch Unberechtigte

Verhaltensregeln:

Organisatorische Maßnahme

9.2. Trennung der Zuordnungsmöglichkeit bei pseudonymisierten Daten

Beschreibung:

Dort wo eine Pseudonymisierung von Daten vorgenommen wird, erfolgt stets eine Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System.

Risiken:

Dateneinsicht durch Unberechtigte

Verhaltensregeln:

Technische Maßnahme

10. Data protection Measurements

10.1. Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

Beschreibung:

Es wird darauf Wert gelegt, dass ein Widerruf technisch so einfach möglich ist wie eine Zustimmung. Zur besseren Kommunikation in datenschutzrechtlichen Angelegenheiten ist dafür auch eine spezielle Email Adresse eingerichtet. Darüber hinaus ist ein Widerruf von Einwilligungserklärungen über an entsprechenden Stellen eingebaute Links möglich.

Risiken:

unrechtmäßige Verarbeitung von Daten, Nicht-Einhaltung von Betroffenenrechten

Verhaltensregeln:

Technische Maßnahme

10.2. Einrichtung einer Stabstelle für Informationssicherheit

Beschreibung:

Es wurde eine Stabstelle geschaffen, welche die Behandlung von Sicherheitsvorfällen und die Abschätzung von Informationssicherheitsrisiken verantwortet. Die notwendige Kenntnisse und Erfahrungen im Bereich der Datensicherheit sind in den jeweiligen Jobprofilen der Mitarbeiter verankert.

Risiken:

Gefahr von Sicherheitslücken, Hackerangriffe, Dateneinsicht von Unberechtigten

Verhaltensregeln:

Organisatorische Maßnahme

10.3. Erfüllung der Informationspflichten

Beschreibung:

Alle Verarbeitungstätigkeiten und betroffene Personenkategorien sind bekannt. Für alle Betroffenen aus einer Datenverarbeitung wurde eine Entscheidung getroffen, wie diese über die Verarbeitung ihrer Daten informiert werden. Die Erfüllung der Informationspflichten gem. Art 13 und 14 DSGVO ist damit sichergestellt. Die Erfüllung der Informationspflichten erfolgt durch die allgemeine Datenschutzerklärung sowie durch die Datenschutzerklärung für MitarbeiterInnen. Bei Bedarf werden auch entsprechende Einzelinformationen erstellt.

Risiken:

unrechtmäßige Verarbeitung von Daten, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

10.4. Mitarbeiter geschult und auf das Datengeheimnis verpflichtet

Beschreibung:

Im Zuge der Unterschrift unter den Dienstvertrag werden Mitarbeiter angehalten auch die Verpflichtung zum Datengeheimnis zu unterschreiben. Mitarbeiter werden über den Inhalt und die Konsequenz eines Verstoßes informiert. Bestehende Mitarbeiter wurden durch eine separate Vereinbarung auf das Datengeheimnis verpflichtet.
Es besteht eine Datenschutz- und Informationssicherheitsrichtlinie im Unternehmen. Darüber werden auch entsprechende Schulungen abgehalten bzw. ein E-Learning angeboten.

Risiken:

Geheimnisbruch, nicht datenschutzkonformes Verhalten

Verhaltensregeln:

Organisatorische Maßnahme

10.5. Prozess zur Abwicklung von Betroffenenprozessen

Beschreibung:

Der Ablauf und die Zuständigkeiten für die Abwicklung von Betroffenenrechten ist klar geregelt. Für die Geltendmachung von Betroffenenrechten ist eine eigene Email-Adresse eingerichtet. Es existiert ein formalisierter Prozess zur Durchführung von Betroffenenrechten. Eine Dokumentation der Betroffenenprozesse erfolgt an zentraler Stelle. Der gesamte Prozess wird über das bestehende Datenschutzmanagement-Tool abgebildet.

Risiken:

nicht datenschutzkonformes Verhalten, Nicht-Einhaltung von Betroffenenprozessen

Verhaltensregeln:

Organisatorische Maßnahme

10.6. Software-Lösungen für Datenschutz-Management im Einsatz

Beschreibung:

Für die Dokumentation des Verarbeitungsverzeichnisses und der technischen / organisatorischen Maßnahmen kommt eine eigene Datenschutzmanagement Software zum Einsatz. Dort werden u.a. auch zentral sämtliche relevante Dokumente zum

Datenschutz gesammelt (insbesondere die Auftragsverarbeitervereinbarungen) sowie auch Betroffenenprozesse und Datenpannen dokumentiert.

Risiken:

nicht datenschutzkonformes Verhalten, nicht datenschutzkonforme Organisation

Verhaltensregeln:

Technische Maßnahme

10.7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Beschreibung:

Verfügbare Sicherheitsupdates werden nach einem Wave-Prinzip bei Server und Clients installiert. Die Ausrollung dieser Updates wird über entsprechende Reports überprüft.
Die Funktionalität der Notstrom-Aggregate für die DataCenter wird regelmäßig überprüft.
Die Wiederherstellung von Backups wird regelmäßig überprüft.
Für extern erreichbare Systeme werden Penetrationtests durchgeführt und dokumentiert.

Risiken:

nicht datenschutzkonformes Verhalten, Unkenntnis von Anweisungen, fehlende Sicherheit bei Datenverarbeitungen

Verhaltensregeln:

Technische Maßnahme

11. Incident-Response-Management

11.1. Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

Beschreibung:

Es wurde eine standardisierte Vorgehensweise zur Behandlung von Sicherheitsvorfällen definiert. Die Abläufe, Prozesse und Vorgaben für verschiedene Sicherheitsvorfälle wurden eindeutig geregelt und geeignet dokumentiert. Dabei ist klar definiert was ein Sicherheitsvorfall ist. Die Definition richtet sich dabei nach dem Schutzbedarf betroffener Geschäftsprozesse, IT-Systeme bzw. Anwendungen. Die Einstufung von Sicherheitsvorfällen wird durch geeignete Personen vorgenommen. Die Vorgehensweise der Meldung von Sicherheitsvorfällen ist allen Mitarbeitern bekannt. Meldewege und Eskalationsstrategien wurden festgelegt. Gegenmaßnahmen zur Eindämmung und Abwehr von Sicherheitsvorfällen werden unverzüglich eingeleitet.

Risiken:

Datenverlust, Hacking, unrechtmäßige Datenverarbeitung

Verhaltensregeln:

Organisatorische Maßnahme

11.2. Dokumentierter Prozess zur Erkennung und Meldung von Datenpannen

Beschreibung:

Das Erkennen und die Behandlung von Datenpannen ist in einer Richtlinie (Datenschutz- und Informationssicherheitsrichtlinie) beschrieben. Die Entdeckung einer Datenpanne (Verletzung des Schutzes personenbezogener Daten) ist immer umgehend der Leitungsebene und der für den Datenschutz zuständigen Person zu melden. Das gilt auch, wenn nur der Verdacht besteht, dass sich eine Datenpanne ereignet hat. Die Leitungsebene unter

Beiziehung der für den Datenschutz verantwortlichen Person beurteilen das Risiko und entscheiden über die Meldepflicht gegenüber der Aufsichtsbehörde und gegenüber den Betroffenen. Die Vorgehensweise bei Datenpannen ist allen Mitarbeitern bekannt. Gegenmaßnahmen zur Eindämmung und Abwehr von Datenpannen werden unverzüglich eingeleitet.

Risiken:

Datenverlust, Hacking, unrechtmäßige Datenverarbeitung

Verhaltensregeln:

Organisatorische Maßnahme

11.3. Einsatz von Spamfiltern und regelmäßige Aktualisierung

Beschreibung:

Es wird Software zum Filtern elektronischer unerwünschter Werbung (Spam) eingesetzt. Der Spamfilter wird periodisch aktualisiert und damit auf den neuesten Stand gebracht.

Risiken:

Hacking, Zugriff von Unberechtigten

Verhaltensregeln:

Technische Maßnahme

12. Privacy-friendly default settings

12.1. Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

Beschreibung:

In entsprechenden Richtlinien ist geregelt, dass jeder Mitarbeiter, bei jeder Datenanwendung zu prüfen hat, ob tatsächlich nur jene Daten verarbeitet werden, die für die Erreichung des Zwecks der Anwendung notwendig ist. Datensparsamkeit und Zweckbindung sind Grundsätze in der Datenverarbeitung innerhalb der Organisation.

Risiken:

fehlende Zweckbindung, unrechtmäßige Verarbeitung von Daten

Verhaltensregeln:

Organisatorische Maßnahme