1 Dokumentenlenkung

1.1 Dokumenteneigenschaften

Inhalt	Technische und organisatorische Maßnahmen
Dokumentenversion	1.2

2 Inhaltsverzeichnis

3 Dokumentation

3.1 Organisation

Die myfactory International GmbH ergreift die folgenden allgemeinen organisatorischen Maßnahmen gem. Art. 25, Art. 32 DSGVO zum Schutz der personenbezogenen Daten:

Alle Mitarbeiter der myfactory International GmbH werden schriftlich auf das Datengeheimnis verpflichtet. Die Mitarbeiter werden mindestens einmal jährlich zu den Themen Datenschutz und Informationssicherheit geschult. Zudem existieren ein Datenschutzkonzept und Regelungen zur Passwortsicherheit, zum Umgang mit personenbezogenen Daten und Informationen und zur Nutzung von IT- und TK-Systemen.

3.2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO), Zutrittskontrolle

Die myfactory International GmbH ergreift die folgenden Maßnahmen um den Zutritt Unbefugter zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, zu verhindern:

Die Geschäftsräume der myfactory International GmbH sind mit einem elektronischen Zutrittskontrollsystem (Interflex) vor unberechtigten Zutritten geschützt. Nur Angestellte der myfactory erhalten eine entsprechende Code-Karte zur Öffnung und Schließung des Zutrittssystems. Ein elektronisches Zutrittskontrollsystem mit Kartenlesern ist auch an der Tiefgarageneinfahrt und den Tiefgaragen-Schleusentüren zu dem Treppenhaus angebracht.

Die Geschäftsräume der myfactory International GmbH befinden sich in einer eigenen Etage die ausschließlich von myfactory genutzt wird. Die Büroräume sind durch zwei Türen mit elektronischer Zutrittskontrolle gesichert. Die Türen können nur mit entsprechender Zutrittskarte oder von innen geöffnet werden. Büroräume in denen Personen mit besonderen Funktionen (insb. Geschäftsführung, Administration, Rechtliches, Personal, Buchhaltung) arbeiten sind zusätzlich mit Zylinderschloss ausgestattet (Need-to-know-Prinzip).

Die Haupteingangstür im Bürogebäude wird ab 20 Uhr verschlossen und kann nur noch von berechtigten Personen geöffnet werden. Der gesamte Außenbereich, inklusive der Parkplatzanlagen, wird Videoüberwacht. Die Aufzeichnungen werden 10 Tage lang vorgehalten.

Alle Server der myfactory International GmbH werden in Rechenzentren der PlusServer GmbH (im Folgenden PlusServer) betrieben. Der Zutritt zum Rechenzentrum erfolgt über ein elektronisches Zutrittskontrollsystem. Zusätzlich kontrollieren Pförtner der PlusServer die Personalien von Besuchern und tragen diese im Besucherbuch ein.

Videokameras sowie Bewegungs-, Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes. Im Alarmfallwerden die für das Gebäude verantwortlichen Mitarbeiter automatisch alarmiert. Zusätzlich ist das Hauptgebäude 24/7 durch Personal besetzt. Auch diesem Personal werden die Alarmmeldungen angezeigt.

3.3 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO), Zugangskontrolle

Die myfactory International GmbH ergreift die folgenden Maßnahmen um die Nutzung von Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, durch Unbefugte zu verhindern:

Jeder Mitarbeiter verfügt über eine eigenes und personalisiertes Benutzerkonto. Alle Benutzerkonten sind mit individuellen Passwörtern gesichert, die jeweils nur dem Inhaber des Benutzerkontos bekannt sind und nicht anderen Personen, auch nicht innerhalb des Unternehmens, mitgeteilt werden dürfen.

Passwörter müssen mindestens 9 Zeichen umfassen und jeweils mindestens einen Groß- und Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten. Die Verwendung von Trivialpasswörtern (z.B. 123456789) wird durch technische Maßnahmen verhindert. Die Passwörter müssen mindestens alle 90 Tage gewechselt werden. Hierbei können jeweils die letzten 5 verwendeten Passwörter nicht erneut genutzt werden. Benutzerkonten werden nach 5 aufeinanderfolgenden, fehlerhaften Anmeldeversuchen automatisch gesperrt. Nach spätestens 15 Minuten Inaktivität werden Benutzerkonten automatisch vom System gesperrt und können anschließend nur nach Eingabe des Benutzerpassworts entsperrt werden. Alle Anmeldevorgänge werden protokolliert.

Als Maßnahmen gegen SQL-Injections werden ParameterQueries verwendet, eine generelle Ersetzungsfunktionen von Parametern eingesetzt und Filterfunktionen für alle Statements in Systemfunktionen mit sofortigem Verbindungsabbruch bei verdächtigen SQL-Aufrufen angewendet.

3.4 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO), Zugriffskontrolle

Die myfactory International GmbH ergreift die folgenden Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Die Nutzung des myfactory-Internetzugangs und der myfactory-E-Mail-Konten ist ausschließlich zu dienstlichen Zwecken zulässig. Mit dieser Maßnahme wird das Risiko für Malware und Drive-By-Infektionen deutlich reduziert. Zusätzlich ist auch die Nutzung der IT- und TK-Systeme selbst ausschließlich zu dienstlichen Zwecken gestattet. Fremdpersonen dürfen diese nicht bedienen.

Das Einbringen von privaten IT- und TK-Systemen, wie zum Beispiel Laptops, Smartphones und USB-Festplatten ist nicht gestattet. Die von der myfactory International GmbH zur Verfügung gestellten Laptops werden für mobile Arbeiten mit Sichtschutzfolien ausgestattet. Die Arbeitsplatzrechner sind vor dem Verlassen des Arbeitsplatzes zu sperren.

Um unautorisierte Zugriffe zu verhindern, sind die Server der myfactory mittels zwei hintereinander geschalteten Firewalls geschützt. Bei der ersten Firewall handelt es sich um eine externe hardwarebasierte Cisco-Firewall, bei der zweiten Firewall um eine softwarebasierte Firewall. Beide Firewalls sind nach dem Default-Deny-Prinzip konfiguriert und verfügen nur über Freigaben, die für den Geschäftsbetrieb zwingend notwendig sind.

3.5 Integrität (Art. 32 Abs. 1 lit. b DSGVO), Weitergabekontrolle

Die myfactory International GmbH ergreift die folgenden Maßnahmen um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder während der temporären Aufbewahrung an einem anderen als den üblichen Speicherort nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Flipcharts und Whiteboards in Besprechungsräumen werden beim Verlassen des Raums entfernt.
Nicht mehr benötigte Papierdokumente (auch Fehldrucke u. -kopien) und Datenträger mit personenbezogen Daten oder anderen vertraulichen Informationen werden unverzüglich und unwiederbringlich vernichtet, sofern keine gesetzlichen oder vertraglich auferlegten Aufbewahrungsfristen entgegenstehen. Papierdokumente werden mit Aktenvernichtern der Sicherheitsstufe P-3 im Kreuzschnittverfahren vernichtet. Datenträger werden von der IT-Abteilung mittels Mehrfachüberschreibung sicher gelöscht.

3.6 Integrität (Art. 32 Abs. 1 lit. b DSGVO), Eingabekontrolle

Die myfactory International GmbH ergreift die folgenden Maßnahmen um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

Die Eingabekontrolle erfolgt über eine ausführliche Protokollierung aller Schreib-, Änderungs- und Löschaktivitäten. Diese Protokollierung umfasst sowohl die Aktivitäten von myfactory-Mitarbeiter, als auch Kundenaktivitäten und wird den Kunden aus Transparenzgründen entsprechend aufbereitet zur Verfügung gestellt. Kunden können jeweils nur die Aktivitäten ihrer eigenen Instanzen einsehen.

3.7 Auftragskontrolle, regelmäßige Überprüfung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Die myfactory International GmbH ergreift die folgenden Maßnahmen um zu gewährleisten, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ausschließlich im Rahmen der Weisungen erfolgen:

Auftragsverarbeiter (im Sinne des Art. 28 DSGVO), wie die PlusServer GmbH, werden in jedem Fall vertraglich zur Einhaltung der geltenden Datenschutzbestimmungen verpflichtet. (Verträge zur Auftragsverarbeitung) Hierzu zählen auch Kontrollrechte der myfactory International GmbH gegenüber den Auftragsverarbeitern und die Dokumentation von Support-Aufträgen. Weiterhin werden alle Auftragsverarbeiter dazu verpflichtet personenbezogene Daten nur nach Weisung der myfactory International GmbH zu erheben, verarbeiten und zu nutzen. Auch Dienstleister der Auftragsverarbeiter (Unterauftragnehmer), müssen im gleichen Maße zur Einhaltung der oben beschriebenen Grundsätze verpflichtet und der myfactory International GmbH direkte Weisungsbefugnisse eingeräumt werden. Diese Weisungs- und Kontrollrechte erstrecken sich ebenfalls auf die Auftraggeber der myfactory International GmbH.

3.8 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Die myfactory International GmbH ergreift die folgenden Maßnahmen um zu gewährleisten, dass Daten gegen zufällige und mutwillige Zerstörung oder Verlust geschützt sind:

Alle Plus-Server-Rechenzentren werden über eine eigene Trafostation mit Strom versorgt. Jedes Server-Rack verfügt über mindestens zwei separate Stromkreisläufe, die alle Gräte redundant mit Strom versorgen und jeweils einzeln mit mindestens 16 Ampere abgesichert sind. Zusätzlich werden viele Geräte mittels zweier separater Netzteile redundant mit Strom versorgt.

Der gesamte Energieverbrauch der Rechenzentren wird über unterbrechungsfreie Stromversorgungsysteme (USV-Systeme) sichergestellt. Im Falle eines Stromausfalls garantiert die USV-Anlage eine unterbrechungsfreie Umschaltung auf eines der Notstrom Dieselaggregate. Daneben filtert die USV-Anlage vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes.

Die Dieselaggregate können bei einem Stromausfall das gesamte Rechenzentrum und die Kühlsysteme konstant mit Energie versorgen. Der Kraftstoffvorrat reich für mindestens 48 Stunden unter Volllast aus. Eine Auftankung ist während des laufenden Betriebs der Generatoren möglich.

Alle Rechenzentren verfügen über ein Wasser- und Brandfrüherkennungssystem. Die Brandmeldeanlage verfügt zudem über eine direkte Aufschaltung an die jeweils örtlich zuständige Feuerwehr. Die Gebäudeaußenhaut ist mittels Überspannungsschutz gegen Blitzschlag abgesichert.

Im Falle von Rauchentwicklung oder eines tatsächlichen Brandes flutet die Brandbekämpfungsanlage innerhalb von 60 Sekunden mit 150fachen Luftdruck die vom Brand betroffenen Bereiche des Rechenzentrums mit Argon (alternativ Inergen). Brände werden so aufgrund des Sauerstoffentzugs schnell und sicher gelöscht, ohne dass es hierbei zu Schäden an der Hardware oder den gespeicherten Daten kommt.

Nachts erstellt PlusServer eine Kopie des kompletten Servers (Snapshot) auf ein separates Backup-System. Die Server-Kopie und das Backup-System befinden sich in einer anderen Brandschutzzone als die von myfactory genutzten Server. (Georedundanz)

Die Kundendaten werden redundant auf einem HotPlug-Raid-System gespeichert, sodass defekte Festplatten ohne Unterbrechung des Betriebs und ohne Datenverluste ausgewechselt werden können.

Mit PlusServer wurde ein 24x7 Service-Vertrag geschlossen, welcher die kurzfristige Behebung technischer Probleme, bis hin zum Austausch eines ganzen Servers beinhaltet.

3.9 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO), Trennungsgebot

Die myfactory International GmbH ergreift die folgenden Maßnahmen um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten voneinander getrennt verarbeitet und nicht zusammengeführt werden.

Die Kundendaten von unterschiedlichen Mandanten werden jeweils in voneinander getrennten Datenbanken gespeichert. (Logische Man
dantentrennung)

Entwicklungs-, Test-, und Produktivsysteme sind streng voneinander getrennt.

3.10 Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Die myfactory International GmbH ergreift die folgenden Maßnahmen um zu gewährleisten, dass eine regelmäßige Überprüfung, Bewertung und Evaluierung stattfindet.

Es ist ein Datenschutz-Management-System (DSMS) implementiert. Es finden Stichprobenkontrollen statt. Daneben bestehen ein Sicherheitskonzept und ein System zum Incident-Response-Management..