mps public solutions gmbh
Maria Trost 1
56070 Koblenz

Anlage 1

Technische und organisatorische Maßnahmen / Datenschutzkonzept

Der Auftragsverarbeiter sichert zu, dass er die nachfolgend beschriebenen Mindestanforderungen im Rahmen seines Datenschutzkonzeptes einhält. Das Datenschutzkonzept beschreibt die im Rahmen der Auftragsverarbeitung erforderlichen Maßnahmen beim Auftragsverarbeiter, um den sicheren Umgang mit personenbezogenen Daten zu gewährleisten. Die Grundlage für dieses Datenschutz-Konzept bilden die EU-Datenschutzgrundverordnung (DS-GVO) und gegebenenfalls weitere von den interessierten Parteien geforderten Maßnahmen. Hierbei orientiert sich der Auftragsverarbeiter im Wesentlichen an den Vorgaben der Artikel 24, 25 und 32 DS-GVO. Auf Anforderung weist der Auftragsverarbeiter die Einhaltung entsprechend nach.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Die Räume, in denen die Verarbeitung personenbezogener Daten erfolgt oder Datenverarbeitungsanlagen installiert sind, sind nicht frei zugänglich. Sie sind bei Abwesenheit der Mitarbeiter verschlossen. Die Zutrittsberechtigungen sind in einem geregelten Verfahren nach dem „need to know Prinzip“ vergeben und werden regelmäßig hinsichtlich ihrer Erforderlichkeit überwacht. Räume, in denen Datenverarbeitungsanlagen (Server, Netzwerkverteiler usw.) untergebracht sind, sind besonders zutrittsgeschützt und nur für Beschäftigte der IT-Administration und der Geschäftsleitung zugänglich. Alternativ sind die Geräte in geeigneten und verschlossenen Schränken untergebracht. Die Zugänge sind Videoüberwacht.

1.2. Zugangskontrolle

Die Zugangskontrolle verhindert, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können. Der Zugang zu den Datenverarbeitungssystemen ist mit Benutzerkennung und einem sicheren Passwort geschützt.
Serversysteme sind nur mit Passwort und über passwortgeschützte, verschlüsselte Verbindung durch Benutzer mit Administratorrechten nutzbar. Clientsysteme sind nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar.

Eine serverseitige Passwortrichtlinie sorgt für die automatische Umsetzung folgender Passwortvorgaben:
Passwörter sind den Komplexitätsanforderungen entsprechend mindestens 12 Zeichen lang. und werden spätestens nach Ablauf von 180 Tagen geändert. Hierbei wird eine Historie der letzten sechs Passwörter gespeichert. Die erneute Verwendung der letzten sechs Passwörter ist ausgeschlossen.
Nach drei fehlerhaften Anmeldeversuchen wird das Konto gesperrt und nur durch einen Administrator wieder freigeschaltet.
Es ist ein verbindliches Verfahren zur Vergabe von Berechtigungen implementiert. Eine eindeutige Zuordnung von Benutzerkonten zu Benutzern ist gewährleistet. Des Weiteren verhindern stets aktuelle Firewall und Virenscanner einen unberechtigten Zugang.

1.3 Zugriffskontrolle

Für die Zugriffe auf personenbezogene Daten ist ein dokumentiertes, rollenbasiertes Berechtigungskonzept vorhanden, welches die Zugriffe in der Form einschränkt, dass nur berechtigte Personen auf die für ihre Aufgabe notwendigen personenbezogenen Daten zugreifen können (Minimumprinzip). Die Passwort-Regelungen aus der Zugangskontrolle sind auch im Rahmen der Zugriffskontrolle umgesetzt. Die administrativen Tätigkeiten sind auf einen kleinen Kreis von Administratoren eingeschränkt. Die Tätigkeiten der Administratoren sind im Rahmen technisch vertretbaren Aufwandes überwacht und protokolliert.

1.4 Trennungskontrolle

Die Trennung von personenbezogenen Daten ist durch unterschiedliche Speicherorte oder durch eine Mandantentrennung sichergestellt.

2. Integrität

2.1 Weitergabekontrolle

Die Weitergabekontrolle gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Die personenbezogenen und sonstigen vertraulichen Daten sind auf unterschiedliche Weise gegen unbefugten Zugriff und gegen unbefugtes Kopieren geschützt.

Beim Datenaustausch mit physikalischen Medien (z.B. Festplatten, USB-Sticks) wird das Verfahren Microsoft® BitLocker mit AES-Verschlüsselung und einer Schlüssellänge von 256 Bit eingesetzt.

Eine elektronische Übertragung geschieht nur verschlüsselt und über sichere Leitungen mit einer zuverlässigen Identifizierung und Authentifizierung der Empfänger. Hier kommt ein SFTP-Server (Secure File Transfer Protocol) der Firma mps mit SSH-Verschlüsselung zum Einsatz.

Am Arbeitsplatz gilt das Prinzip des aufgeräumten Schreibtischs (*Clean-Desk-Prinzip*), d.h. jeder ist verpflichtet und dafür verantwortlich, personenbezogene Daten und vertrauliche Informationen und Datenträger mit entsprechenden Daten in seinem Bereich - insbesondere bei Abwesenheit und nach Geschäftsschluss - sicher und ordnungsgemäß aufzubewahren (in verschlossenen Schränken und Schreibtischen, passwortgesichertem PC etc.).

Vertrauliche Unterlagen sowie Datenträger werden datenschutzkonform vernichtet: Für Papierunterlagen wird ein Schredder mit der Sicherheitsstufe P5 verwendet, Zur Vernichtung elektronischer Daten wird eine sichere Löschung vorgenommen. Ausgesonderte Datenträger werden durch ein externes Unternehmen fachgerecht vernichtet.

2.2 Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
Eingabe oder Veränderung von personenbezogenen Daten sind nach den sich aus der Schutzstufe und den Schutzzielen ergebenden Anforderungen protokolliert.
Alle Mitarbeiter/-innen sind auf das Datengeheimnis, bzw. Fernmeldegeheimnis und Sozialgeheimnis verpflichtet worden.

2.3 Auftragskontrolle

Im Rahmen der Auftragskontrolle ist sichergestellt, dass die im Auftrag durchgeführten Datenverarbeitungsvorgänge ausschließlich auf Weisung des Auftraggebers erfolgen. Hierzu sind die mit der Datenverarbeitung Beschäftigten geschult und unterwiesen. Die Auftragsverarbeitung wird durch interne Kontrollen überwacht. Die Ergebnisse der Kontrollen werden dokumentiert.

Subunternehmer können nur auf Basis der mit dem Auftraggeber vereinbarten Regelungen beauftragt werden. Die Prüfpflicht des Auftragnehmers gegenüber seinem Subunternehmer ergibt sich aus der mit dem Auftraggeber abgeschlossenen Vereinbarung zur Auftragsverarbeitung.

3. Verfügbarkeit und Belastbarkeit

Die Verarbeitung von personenbezogenen Daten erfolgt auf Datenverarbeitungssystemen, die einem regelmäßigen und dokumentierten Patch-Management unterliegen. Es sind im Netz keine Systeme verbunden, die außerhalb der Wartungszyklen der Hersteller sind. Sicherheitsrelevante Patches werden schnellstmöglich nach Bekanntgabe installiert.

Die durchgängige Verfügbarkeit von personenbezogenen Daten ist mittels redundanten Speichermedien und Datensicherungen gemäß dem Stand der Technik gewährleistet. Rechenzentren und Serverräume entsprechen dem Stand der Technik (Temperaturregelung, Brandschutz, etc.). Die Server verfügen über eine

unterbrechungsfreie Stromversorgung (USV), die ein geregeltes Herunterfahren ohne Datenverlust sicherstellen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es ist ein Verfahren zur Überwachung des Datenschutzes im Unternehmen implementiert. Dieses beinhaltet die Verpflichtung der Beschäftigten auf das Datengeheimnis, die Schulung und Sensibilisierung der Beschäftigten und die regemäßige Auditierung der Datenverarbeitungsverfahren. Ebenso erfolgt die Dokumentation des für den Auftraggeber durchgeführten Verarbeitungsverfahrens vor Aufnahmen der Datenverarbeitung. Für Datenschutzverletzungen und die Wahrung der Betroffenenrechte ist ein durchgängiger Melde- und Bearbeitungsprozess eingeführt. Dieser beinhaltet auch die Information des Auftraggebers.