Technische und organisatorische Maßnahmen zur Datensicherheit bei cojama Infosystems GmbH gem. Art. 32 Abs. 1, Art. 25 Abs. 1 DS-GVO

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind:

1. Vertraulichkeit

1.a Zutrittskontrolle

Die technische Infrastruktur für das Hosting der Kundensysteme ist im Hochverfügbarkeits-Rechenzentrum der Betreiber-Gesellschaft Digital Frankfurt GmbH in Frankfurt / Main untergebracht.

Folgende Maßnahmen verhindern den Zutritt unbefugter Personen zu den Datenverarbeitungssystemen von cojama:

- Verschlossene Außentüren des Gebäudes
- Umzäunung des Grundstücks
- Verschlossene Türen zu den Gebäudeabschnitten / Sicherheitszonen

  (Chipkarten und elektr. Türöffner)
- Nummernschlösser an den einzelnen Racks
- Kameraüberwachung im Innen- und Außenbereich
- Permanent besetzte Sicherheitszentrale
- Zutritt nur für
  - dauerhaft akkreditierte Mitarbeiter von cojama
  - durch cojama avisierte Personen, die sich mittels gültigem Personalausweis oder Reisepass ausweisen und vorher namentlich angemeldet wurden
- Die elektronischen Schlüssel zu den Gebäudeabschnitten müssen bei Verlassen des Hauses abgegeben werden.
- Dokumentation mit Zeitstempel bei Ankunft und Verlassen

Die technische Infrastruktur für die interne Bürokommunikation von cojama ist in der Geschäftsstelle in Fulda untergebracht.

Folgende Maßnahmen verhindern den Zutritt unbefugter Personen zu den Datenverarbeitungssystemen von cojama:

- Verschlossene Außentüren des Gebäudes
- Verschlossene Türen zu den Gebäudeabschnitten
- Einbruchmeldeanlage
- Zutritt nur für interne Mitarbeiter von cojama
- Gäste erhalten nur in Begleitung eines Mitarbeiters Zutritt zu den Räumlichkeiten

1.b Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

- Alle Serversysteme sind durch Firewall-Appliances zum Internet und zu den Netzen anderer Kunden geschützt.
- Firewalls und Server erhalten regelmäßig Security-Patches.
- Der Client-Zugriff erfolgt ausschließlich SSL-verschlüsselt.
- Nur ein kleiner, sorgfältig ausgewählter Personenkreis besitzt administrative Zugangsberechtigungen.
- Administratoren arbeiten mit personalisierten Benutzerkonten, die einzeln gesperrt werden können.
- Keines der betriebenen Serversysteme besitzt eine Netzwerkschnittstelle außerhalb von Netzen, die durch eine Firewall vom Internet getrennt sind.
- In den Management-Netzen befinden sich keine Netzwerkschnittstellen von Kunden-Servern.
- Grundsätzlich ist kein IP-Port der Server vom Internet oder von einem anderen produktiven VLAN aus erreichbar. Es werden nur die für den Zugriff auf die jeweilige Anwendung erforderlichen Ports geöffnet.

1.c Zugriffskontrolle

Maßnahmen die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung 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.:

- Jeder Anwender erhält ein personalisiertes Benutzerkonto, das nur den Zugriff auf das eigene Postfach, die entsprechende SharePoint-Seite oder sonstige bereitgestellte Ressourcen erlaubt.
- Das Benutzerkonto ist durch ein Kennwort geschützt (Mindestlänge 8 Zeichen sowie Komplexitätsanforderungen), das der Anwender selbst ändern kann. Nach 10-maliger Falscheingabe wird das Benutzerkonto für 30 Minuten gesperrt (Account-Lock-Out).
- Account-Lock-Out-Ereignisse werden protokolliert.

1.d Trennungskontrolle

Maßnahmen, mit denen sichergestellt wird, dass Mandanten, die auf einer gemeinsamen Hosting-Infrastruktur untergebracht sind, weder Kenntnis von der Existenz, noch den Daten eines anderen Mandanten erhalten:

- Die Benutzerobjekte eines Kunden befinden sich in einer eigenen Organisationseinheit (OU) des übergreifenden Verzeichnisdienstes (ActiveDirectory). Das ActiveDirectory ist für das Hosting mehrerer Mandanten konfiguriert.
- Die Hosted-Exchange Infrastruktur ist ebenfalls für das Hosting mehrerer Mandanten konfiguriert. Jeder Kunde erhält einen eigenen Satz Adresslisten, die den Benutzern unter Verwendung von Adressbuchrichtlinien zugewiesen werden. Somit ist sichergestellt, dass Benutzernamen für andere Kunden nicht sichtbar sind.
- Eine Website-Sammlung innerhalb von Hosted-SharePoint ist fest mit der Organisationseinheit des entsprechenden Kunden im ActiveDirectory assoziiert. Somit können nur Benutzer des jeweiligen Kunden ausgewählt werden, um ihnen Zugriffsberechtigungen auf eine SharePoint Seite zu erteilen.
- Serversysteme, die dediziert für einen Kunden betrieben werden, befinden sich in einem Netzwerk-Segment (VLAN), das exklusiv dem jeweiligen Kunden zur Verfügung steht. Jedes dieser VLANs ist durch Firewall-Systeme von den VLANs anderer Kunden und dem Internet getrennt.
- Das zentrale Verwaltungssystem, welches den Kunden ein Web-Interface u. a. für das Management von Benutzerkonten zur Verfügung stellt, verwendet Zugriffskontrolllisten (ACL) für die Realisierung der Mandantentrennung.

1.e Pseudonymisierung

Die Bezeichnungen der einzelnen Hosting-Kunden werden an folgenden Stellen durch die Verwendung einer eindeutigen Organisations-ID pseudonymisiert:

- Organisationseinheiten (OUs) innerhalb des Hosting-ActiveDirectory
- Objekte der virtuellen MS Exchange-Organisationen (Adresslisten, Adressbuchrichtlinien, etc.)
- Verzeichnisse für individuelle SharePoint Datensicherungen
- Datenbank-Namen für dedizierte SharePoint Server
- Technische Benutzerkonten für dedizierte SharePoint Server

2. Integrität

2.a Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- SSL / TLS-Verschlüsselung der Kommunikation zwischen Client und Server
- SSL / TLS-Verschlüsselung der E-Mail Übertragung (SMTP) von und zu entfernten Mailservern, sofern diese Verschlüsselung unterstützen.
- E-Mails mit personenbezogenen Daten werden von cojama-Mitarbeitern nur verschlüsselt versandt.
- Für den gesamten Datenverkehr zwischen cojama-Geschäftsstelle und Rechenzentrum kommt ein VPN zum Einsatz.
- Ein Transport von Datenträgern erfolgt im regulären Betriebsablauf nicht.

2.b Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

- Die Security-Eventlogs der Serversysteme werden wöchentlich archiviert.
- Darin enthalten sind an personenbezogenen Informationen An- und Abmeldevorgänge von Benutzern sowie fehlerhafte Kennwort-Eingaben durch Benutzer.
- Wird ein Benutzerkonto auf Grund mehrmaliger Falscheingabe des Kennworts gesperrt, so wird automatisch eine Information an die cojama-Administratoren generiert.
- Die Nutzung der Hosting-Produkte durch die Anwender wird protokolliert. Die entsprechenden Protokolle werden ausschließlich zur Fehlerdiagnose verwendet. Eine Verhaltenskontrolle der Betroffenen findet nicht statt.
- Im Übrigen liegt die Verantwortung für die Dateneingabe bei allen Hosting-Produkten auf Seiten des Kunden.

3. Verfügbarkeit und Belastbarkeit

3.a Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind und die Verfügbarkeit von Systemen und Anwendungen sicherstellen:

- Trennung der Lokationen für Produktiv- und Backup-Systeme
- Sicherheitsmaßnahmen gegen Feuer, Diebstahl und Ausfall der Netzspannung.
- Tägliche Sicherung aller Serversysteme, Datenbanken, etc., Aufbewahrungsdauer min. zwei Wochen
- Ausstattung aller Server mit fehlertoleranten Massenspeicher-Systemen.
- Betrieb der Anwendungen in hochverfügbarer Konfiguration
- Redundante Auslegung der Netzwerk-Infrastruktur (Teaming, Multi-Carrier-Anbindung, etc.)
- Betrieb der Firewall im Cluster

- Überwachung von Hardware, Serversystemen, Netzwerkkomponenten und Anwendungen mit entsprechender Alarmierung
- Durch den Benutzer gelöschte Elemente innerhalb von Exchange-Postfächern und SharePoint Seiten werden 30 Tage lang auf dem Produktivsystem aufbewahrt, bevor sie endgültig gelöscht werden. Die Wiederherstellung kann nur durch den Benutzer selbst erfolgen.
- Malware-Schutz des gesamten E-Mail Verkehrs (Hosting-Produkte und E-Mail-Adressen der cojama)
- Dokumentation von Strukturen und Veränderungen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.a Datenschutz-Management

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig überprüft und bewertet, um die Sicherheit der Verarbeitung gem. Art. 32(1) DS-GVO auf Dauer zu gewährleisten.

Die regelmäßige Evaluierung von Verarbeitungsverfahren und Datensicherheitsmaßnahmen wird dokumentiert.

4.b Incident-Response-Management

Ausfall-Ereignisse und Sicherheitsvorfälle werden dokumentiert.

Vorfälle werden unverzüglich an den betroffenen Auftraggeber gemeldet

Information im Vorfeld geplanter Wartungsarbeiten werden auf der Website veröffentlicht.

Einschränkungen der Dienstqualität oder Verfügbarkeit werden auf der Website veröffentlicht, sofern zu erwarten ist, dass keine kurzfristige Behebung möglich ist.

Cojama-Mitarbeiter sind sensibilisiert und auf das Incident-Management geschult.

4.c Datenschutzfreundliche Voreinstellungen

Da die angebotenen Dienste im Wesentlichen dem Bereich IT-Infrastruktur zuzuordnen sind, liegt die Entscheidung darüber, welche Daten darin gespeichert werden, beim Auftraggeber.

Die angebotenen Dienste dienen nicht der gezielten Erfassung bestimmter Daten.

Dienste wie E-Mail Archivierung oder längere Backup-Aufbewahrungszeiten erfordern eine gesonderte Beauftragung.

4.d Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Alle Dienstleister, die für den Auftragnehmer Daten in dessen Auftrag verarbeiten, Einfluss auf die Verfügbarkeit der Systeme haben oder Zugriff auf personenbezogene Daten erlangen können, werden sorgfältig ausgewählt.

Diese werden gem. Art. 28 DS-GVO vertraglich an den Auftragnehmer gebunden.

— Beim Auftragnehmer ist als Beauftragter für den Datenschutz schriftlich benannt:

Herr Frank Spaeing
c/o cojama Infosystems GmbH
Flemingstr. 10
36041 Fulda
E-Mail: datenschutz@cojama.com