NETWAYS WEB SERVICES

TOM-ANLAGE

Anlage der technischen und organisatorischen Maßnahmen (TOM) i.S.d. Art. 32 DS-GVO

Gültig für die NETWAYS Managed Services GmbH

NETWAYS Managed Services GmbH | Deutschherrnstr. 15-19 | 90429 Nürnberg
nws.netways.de | Tel. +49 911 92885-0 | info@netways.de

Geschäftsführer: Julian Hein, Bernd Erk, Sebastian Saemann
Registergericht Nürnberg HRB18461 | Steuernummer USt.-ID: DE 216837402

In Verbindung mit dem Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO verpflichten sich die Vertragsparteien – der Verantwortliche und der Auftragsverarbeiter - in ihrem jeweiligen Verfügungsbereich und bezogen auf den Vertragsgegenstand, gem. Art. 28 Abs. 3 lit. c DS-GVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, durch geeignete technische und organisatorische Maßnahmen ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Im Einzelnen handelt es sich hierbei um folgende Maßnahmen:

1. VERTRAULICHKEIT GEM. ART. 32 ABS. 1 LIT. B DS-GVO

1.1 ZUTRITTSKONTROLLE

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Der Zugang zu den Lokationen ist ausschließlich in Begleitung eines NETWAYS Mitarbeiters erlaubt und der Zutritt ist ausschließlich mit personalisierten Chipkarten, ggf. mit biometrischer Überprüfung oder elektronischem Codeschloss sowie durchgehender Kameraüberwachung möglich. Ein durchgehender Perimeterschutz ist durch Einfriedungsanlagen und Personal gewährleistet.

Einzelne Verarbeitungsanlagen (Racks) sind zusätzlich durch manuelle Schließsysteme gesichert welche mit Tresoren verwaltet werden. Entsprechende Schlüsselregelung inklusive Zugriffsbeschränkung sind implementiert.

1.2 ZUGANGSKONTROLLE

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Die Sicherung von Server- und Clientsystemen erfolgt durch Login mit Benutzername und Passwort. Ein Fernzugriff wird für Konsolen- und VPN-Zugänge mindestens durch asymmetrische Verschlüsselungsverfahren gesichert durchgeführt. Portzugriffe auf exponierte Dienste werden durch redundante Firewall-Systeme / Netzwerkgeräte eingeschränkt. Zentralverwaltete Benutzerberechtigungen, Richtliniensystem für die Einhaltung des Datenschutzes, Passwortvergaberichtlinie, arbeitsrechtliche Geheimhaltungsvereinbarungen und Konsolenunterweisung sind implementiert.

1.3 ZUGRIFFSKONTROLLE

Es ist Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung 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.

Verschlüsselungsqualität und Sicherheitsprotokolle werden nach der Möglichkeit des Auftraggebers implementiert. Grundsätzlich sind Server bzw. allgemein Netzwerkdienste aus dem Internet nicht erreichbar.

Die Anzahl der Administratoren ist auf ein Minimum beschränkt und Benutzerprofile durch ein zentrales Berechtigungssystem verwaltet. Änderungen können durch revisionssichere Snapshots des Festplattenspeichers, ein zentrales Log- oder Konfigurationsmanagement System nachvollzogen werden.

Token- und VPN Zugangssysteme werden durch Tresor- und Zugriffsregelungen geschützt. Vernichtung und Löschung gemäß DIN 66399 und DIN 32757 in den Sicherheitsstufen P5 und T4 auf Wunsch des Auftraggebers. Löschkonzept auf Anfrage einsehbar.

1.4 TRENNUNGSKONTROLLE

Es ist Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Werden Konfigurations-Management oder virtuelle Ressourcen des Auftragnehmers in Anspruch genommen, so sind diese einer Funktionstrennung unterzogen und durchlaufen Test- und Produktionsphase.

Vom Auftragnehmer werden für die Speicherung der Daten nur eigene, physische Möglichkeiten zur Verfügung gestellt. Die logische Trennung der Daten liegt in der Verantwortung des Auftraggebers.

1.5 PSEUDONYMISIERUNG (ART. 32 ABS. 1 LIT. A DS-GVO)

„Pseudonymisierung" bezeichnet die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen.

Eine Pseudonymisierung erfolgt auf Weisung des Auftraggebers entsprechend der Weitergabekontrolle (2.1) oder ggf. im Rahmen einer Sicherung (Privacy by Design). Interne Richtlinien, personenbezogene Daten im Falle einer Weitergabe zu anonymisieren / pseudonymisieren sind implementiert.

2. INTEGRITÄT GEM. ART. 32 ABS. 1 LIT. B DS-GVO

2.1 WEITERGABEKONTROLLE

Es ist Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Der Auftraggeber bekommt eine dedizierte, verschlüsselte Zugriffsmöglichkeit für seine Umgebung welche ggf. in einem eigenständigen VLAN betrieben wird.

Für einmaligen Transport oder Support werden verschlüsselte Verbindungen bereitgestellt, z.B. HTTPS oder SFTP. Eine Speicherung auf Datenträger für den Transport wird nur auf ausdrücklichen Wunsch des Auftraggebers vorgenommen und kann nur durch persönliche Übergabe geschehen. Jeder außerordentliche Transport wird vorher durch den Auftraggeber angeordnet und entsprechend dokumentiert. Weiterhin können ggf. Verschlüsselung und Pseudonymisierung vereinbart werden.

2.2 EINGABEKONTROLLE

Es ist Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Es werden von virtuellen Ressourcen, Serversystemen oder Containern revisionssichere Snapshots des Festplattenspeichers angelegt. Ggf. können Änderungen durch ein zentrales Log-Management System nachvollzogen werden. Änderungen und Eingaben werden durch den Auftraggeber eingestellt und entsprechend dokumentiert.

3. VERFÜGBARKEIT UND BELASTBARKEIT GEM. ART. 32 ABS. 1 LIT. B DS-GVO

3.1 VERFÜGBARKEITSKONTROLLE

Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vermietete Server-Systeme des Auftraggebers sind mit redundanten Plattensubsystemen ausgestattet (Mindestanforderung RAID1) und ggf. mit einem Supportvertrag des Serverherstellers versehen. Die Stromversorgung ist redundant ausgelegt und durch USV / Generatoren gegenüber Ausfällen des EVU geschützt.

Der Auftragnehmer betreibt ein Datensicherungssystem welches ggf. durch den Auftragnehmer genutzt werden kann. Die Sicherung wird standardmäßig einmal am Tag durchgeführt, wobei einmal pro Woche eine Vollsicherung, an den verbleibenden Tagen eine differentielle Sicherung durchgeführt wird. Das Datensicherungssystem wird als verteiltes System ggf. über zwei Standorte betrieben und einer regelmäßigen Überprüfung unterzogen.

Virtuelle Server Systeme und Container werden ggf. per revisionssichere Snapshots des Festplattenspeichers auf das oben beschriebene System gesichert. Die Aufbewahrungszeit beträgt 7 Tage.

4. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG GEM. ART. 32 ABS. 1 LIT. D DS-GVO UND ART. 25 ABS. 1 DS-GVO

4.1 DATENSCHUTZ-MANAGEMENT

Gewährleistung der Nachhaltigkeit des Datenschutzes.

Dokumentation des Datenschutzes vorhanden mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf. Regelmäßige Überprüfung der Wirksamkeit erforderlicher Schutzmaßnahmen wird durchgeführt. Die Mitarbeiter sind geschult auf Vertraulichkeit und sind dem Datengeheimnis verpflichtet.

Der Auftragnehmer kommt den Informationspflichten nach Art. 13 und 14 DS-GVO nach.
Interner Datenschutzbeauftragter im Unternehmen: **datenschutz@netways.de**

4.2 INCIDENT-RESPONSE-MANAGEMENT

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Der Auftragnehmer setzt Firewall-, Netzwerk- und Spamfiltersysteme in redundanter Form für Umgebungen des Auftragnehmers ein. Die Funktionsweise wird durch regelmäßige Kontrolle und Wartung sichergestellt. Projekte und Umgebungen des Auftraggebers werden dokumentiert und der aktuelle Verlauf oder allgemeine Informationen in einem Ticketsystem protokolliert. Sicherheitsvorfälle werden dokumentiert und ein DSB mit einbezogen.

4.3 DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN (ART. 25 ABS. 2 DS-GVO)

Privacy by design / Privacy by default

Es werden nicht mehr personenbezogene Daten erhoben, bearbeitet oder verwendet als für den jeweiligen Zweck erforderlich. Eine einfache Ausübung des Widerrufsrechts des Betroffenen ist möglich.

4.4 AUFTRAGSKONTROLLE

Es ist eine weisungsgemäße Auftragsverarbeitung zu gewährleisten.

Alle Weisungen des Auftraggebers erfolgen schriftlich per E-Mail an unser Ticketsystem, wodurch eine lückenlose Nachvollziehbarkeit gewährleistet ist. Mündliche Absprachen werden im Ticketsystem protokolliert und dem Auftraggeber zur Kontrolle übersendet. Arbeitsanweisungen werden durch Mitarbeiter des Auftragnehmers einer Plausibilitätsprüfung unterzogen. Die Mitarbeiter unterliegen einer Geheimhaltungsvereinbarung. Alle Prozesse werden von den jeweiligen Abteilungsleitern und der Geschäftsführung regelmäßig überprüft und bewertet.

Der Auftragnehmer gewährleistet jederzeit eine einfache Wahrnehmung der Kontrollrechte des Auftraggebers, um das Schutzniveau regelmäßig zu überprüfen.

Es werden grundsätzlich keine weiteren Subunternehmer beauftragt, sofern nicht auf ausdrücklichen Wunsch des Auftraggebers.

Nach Beendigung des Vertrages werden alle Daten des Auftraggebers übergeben oder gelöscht. Ein Löschkonzept kann auf Anfrage eingesehen werden.