Übergreifende technische und organisatorische Maßnahmen (TOM) nach DSGVO

Die folgenden technischen und organisatorischen Maßnahmen zur Datensicherheit werden gemäß Art. 32 DSGVO durch den Auftragnehmer NANICOM e.K., vertreten durch Herrn Sasa Karapandzic, umgesetzt. Diese Maßnahmen sind Bestandteil der Rahmenvereinbarung zur Auftragsverarbeitung.

1. Auftragnehmer

NANICOM e.K.
Champagne 6, 42781 Haan
Vertreten durch Herrn Sasa Karapandzic

2. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b) DSGVO

2.1 Zutrittskontrolle

Es werden Maßnahmen ergriffen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, Büroräumlichkeiten und Serverräumen zu verwehren, die personenbezogene Daten verarbeiten oder nutzen. Dazu gehören automatische Zutrittskontrollsysteme, Alarmanlagen sowie Kameraüberwachung. IT-Anlagen wie Server und Netzwerktechnik werden in verschließbaren und überwachten Räumen gesichert mit Zutrittskontrolle.
Gebäudezugang erfolgt über ein manuelles Schließsystem. Die Ausgabe und Rückgabe der Schlüssel wird schriftlich in Personalverwaltung dokumentiert. Besucher dürfen die Büroräume nur in Begleitung betreten. Reinigungskräfte haben keinen Zutritt zu IT-Anlagen oder Schränken mit personenbezogenen Daten.

2.2 Zugangskontrolle

Um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden, wird eine Zugangskontrolle implementiert. Dies umfasst Passwortschutz. Alle Arbeitsrechner sind verschlüsselt, um die Daten vor Missbrauch zu schützen. Benutzer authentifizieren sich mit komplexen Kennwörtern und Zwei-Faktor-Authentifizierung (2FA). Bei Ausscheiden eines Mitarbeiters werden Zugänge umgehend gesperrt.
Der Zugriff auf IT-Systeme wird durch Firewalls überwacht und eine Antivirus-Software ist ständig aktiv. Remote-Zugriffe erfolgen über gesicherte VPN-Verbindungen.

2.3 Zugriffskontrolle

Zugriffsbeschränkungen stellen sicher, dass nur autorisierte Personen auf personenbezogene Daten zugreifen. Berechtigungskonzepte regeln, welche Mitarbeiter auf welche Daten zugreifen dürfen. Berechtigungen werden bei Änderungen, wie dem Ausscheiden eines Mitarbeiters, sofort angepasst. Alle Zugriffe auf Systeme und Anwendungen werden protokolliert und regelmäßig überprüft. Festplatten von Laptops sind sowohl mit AV-Software ausgestattet wie auch verschlüsselt.

2.4 Trennung

Daten, die für unterschiedliche Zwecke erhoben werden, werden physisch oder logisch getrennt verarbeitet. Dies kann durch separate Datenbanken, virtuelle Maschinen oder differenzierte Berechtigungssysteme erfolgen.

2.5 Pseudonymisierung gem. Art. 32 Abs. 1 lit. a) und Art. 25 Abs. 1 DSGVO

Personenbezogene Daten werden, wo möglich, pseudonymisiert. Dadurch ist es Dritten nicht möglich, Daten einer spezifischen Person zuzuordnen. Die Zuordnungsinformationen werden getrennt und gesichert aufbewahrt. Die Pseudonymisierung findet nur in bestimmten Anwendungsfällen statt, die mit dem Auftragsnehmer vor Übertragung von Daten ausgehandelt werden.

3. Integrität gem. Art. 32 Abs. 1 lit. b) DSGVO

3.1 Eingabekontrolle

Es wird sichergestellt, dass nachvollziehbar ist, wer personenbezogene Daten in das System eingegeben, verändert oder gelöscht hat. Diese Eingaben werden auf verschiedenen Ebenen protokolliert, etwa auf Betriebssystem-, Netzwerk- oder Anwendungsebene. Protokolle werden regelmäßig überprüft und nach sechs Monaten gelöscht.

3.2 Weitergabekontrolle

Personenbezogene Daten werden bei Übertragung, Transport oder Speicherung durch Verschlüsselung geschützt. Zur Sicherstellung der Vertraulichkeit wird die Übermittlung von Daten in Cloud-Systemen wie Microsoft ausschließlich in europäischen Rechenzentren durchgeführt. VPN-Verbindungen und sichere Datenportale werden genutzt, um die Weitergabe zu schützen.

4. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b) DSGVO

4.1 Verfügbarkeit

Maßnahmen wie unterbrechungsfreie Stromversorgung (USV), Datensicherungen und Überspannungsschutz verhindern Datenverlust. Die Daten werden regelmäßig in Rechenzentren gesichert. Daten auf Laptops, die zur Auftragserfüllung benötigt werden, sind lokal verschlüsselt. Zudem werden personenbezogene Daten in europäischen Cloud-Systemen (wie Microsoft Azure)

gespeichert, die in europäischen Rechenzentren betrieben werden, um die DSGVO-Konformität zu gewährleisten.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d) und Art. 25 Abs. 1 DSGVO

5.1 Datenschutz-Management

Die Geschäftsführung ist verantwortlich für Datenschutz und Informationssicherheit. Alle Beschäftigten werden regelmäßig sensibilisiert und auf Vertraulichkeit verpflichtet. Technische und organisatorische Maßnahmen werden jährlich überprüft.

5.2 Incident-Response-Management

Zur Erkennung und Reaktion auf Sicherheitsvorfälle werden Firewalls, Spamfilter und Virenscanner eingesetzt. Notfallpläne für Sicherheitsvorfälle existieren und werden regelmäßig aktualisiert.

5.3 Datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DSGVO

Beschäftigte sind verpflichtet, nur notwendige personenbezogene Daten zu verarbeiten. Standardmäßig werden Benutzerrechte eingeschränkt vergeben.

5.4 Auftragskontrolle

Es wird sichergestellt, dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Der Auftragnehmer verpflichtet alle Unterauftragnehmer zur Einhaltung der DSGVO.

6. Technische und organisatorische Maßnahmen bei Subunternehmen und Cloud-Diensten

Subunternehmer, die in die Verarbeitung personenbezogener Daten eingebunden sind, werden sorgfältig ausgewählt und regelmäßig überprüft. Bei der Nutzung von Cloud-Diensten, insbesondere Microsoft 365, wird sichergestellt, dass die Daten in europäischen Rechenzentren gespeichert und verarbeitet werden.