Anhang 1 zur Vereinbarung zur Auftragsverarbeitung - Technische und Organisatorische Sicherheitsmaßnahmen gemäß Art 32 DSGVO

Version 1.0

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind.

Festlegung von Sicherheitsbereichen

- Realisierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung Zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Begleitung von Fremdpersonal
- Überwachung der Räume

1.2 Zugangskontrolle

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

- Festlegung des Schutzbedarfs
- Zugangsschutz
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Umsetzung einfacher Authentisierung per Username Passwort
- Protokollierung des Zugangs
- Monitoring bei kritischen IT-Systemen
- Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
- Festlegung befugter Personen
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
- Automatische Zugangssperre und Manuelle Zugangssperre

1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Erstellen eines Berechtigungskonzepts
- Umsetzung von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen

WebDesign • ContentManagment • WebHosting • Netzwerktechnik • Datenbanken • Telekommunikation

neTTworker.com
Matthias Rüsseler
Schütterberg 15
25524 Itzehoe

Telefon 04821 / 4078 383
Telefax 04821 / 4078 385

Notruf 04821 / 14 900 15

Internet
www.neTTworker.com
e-mail
info@neTTworker.com

Bankverbindung
Postbank Hannover
BLZ 250 100 30
Konto 2745 33 303

BIC PBNKDEFFXXX
IBAN DE58250100300274533303
St.Nr. 18 072 01621
Gerichtsstand ist Itzehoe

1.4 Verwendungszweckkontrolle

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

• Datensparsamkeit im Umgang mit personenbezogenen Daten
• Getrennte Verarbeitung verschiedener Datensätze
• Regelmäßige Verwendungszweckkontrolle und Löschung
• Trennung von Test- und Entwicklungsumgebung

1.5 datenschutzfreundliche Voreinstellungen

• Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der Betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu gewährleisten, 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.

• Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
• Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
• Protokollierung von Übermittlungen gemäß Protokollierungskonzept
• Sichere Datenübertragung zwischen Server und Client
• Sicherung der Übertragung im Backend
• Sichere Übertragung zu externen Systemen
• Risikominimierung durch Netzseparierung
• Implementation von Sicherheitsgateways an den Netzübergabepunkten
• Härtung der Backendsysteme
• Beschreibung der Schnittstellen
• Umsetzung einer Maschine-Maschine-Authentisierung
• Sichere Ablage von Daten, inkl. Backups
• Gesicherte Speicherung auf mobilen Datenträgern
• Einführung eines Prozesses zur Datenträgerverwaltungen
• Prozess zur Sammlung und Entsorgung
• Datenschutzgerechter Lösch- und Zerstörungsverfahren
• Führung von Löschprotokollen

2.2 Eingabekontrolle

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

• Protokollierung der Eingaben
• Dokumentation der Eingabeberechtigungen

WebDesign • ContentManagment • WebHosting • Netzwerktechnik • Datenbanken • Telekommunikation

3. Verfügbarkeit, Belastbarkeit, Desaster Recovery

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

- Brandschutz
- Redundanz der Primärtechnik
- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Monitoring
- Resourcenplanung und Bereitstellung
- Abwehr von systembelastendem Missbrauch
- Datensicherungskonzepte und Umsetzung
- Regelmäßige Prüfung der Notfalleinrichtungen

3.2 Desaster Recovery – Rasche Wiederherstellung nach Zwischenfall Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

- Notfallplan
- Datensicherungskonzepte und Umsetzung

4. Datenschutzorganisation

- Festlegung von Verantwortlichkeiten
- Umsetzung und Kontrolle geeigneter Prozesse
- Melde- und Freigabeprozess
- Umsetzung von Schulungsmaßnahmen
- Verpflichtung auf Vertraulichkeit
- Regelungen zur internen Aufgabenverteilung
- Beachtung von Funktionstrennung und –zuordnung
- Einführung einer geeigneten Vertreterregelung

5. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl weiterer Auftragnehmer nach geeigneten Garantien
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Informationssicherheitsmanagement nach ISO 27001
- Prozess zur Evaluation der Technischen und Organisatorischen Maßnahmen
- Prozess Sicherheitsvorfall-Management
- Durchführung von technischen Überprüfungen

WebDesign • ContentManagment • WebHosting • Netzwerktechnik • Datenbanken • Telekommunikation