DOKUMENTATION DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

gem. Anlage zu Art. 32 DSGVO

V 1.1

Host Europe GmbH

Hansestr. 111

51149 Köln

1. Präambel

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, treffen der Auftraggeber und der Auftragnehmer die nachfolgenden technischen und organisatorischen Maßnahmen (TOM). Diese gelten für die im Hauptvertrag definierten IT-Leistungen, welche in den unter Ziffer 2 definierten Rechenzentren erbracht werden.

Bei der Auswahl der Maßnahmen wurden die vier Schutzziele des Art. 32 Abs. 1 b) DSGVO, namentlich die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, berücksichtigt. Eine rasche Wiederherstellung nach einem physischen oder technischen Zwischenfall ist gewährleistet. Alle technischen und organisatorischen Maßnahmen werden regelmäßig gemäß Art. 32 Abs. 1 d) DSGVO auf ihre Wirksamkeit hin geprüft.

Generell gilt es folgendes zu beachten:

Die Host Europe GmbH vermietet die Datenverarbeitungsanlage an den Kunden. Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung. Der Kunde entscheidet allein und ausschließlich darüber, welche personenbezogene Daten in welcher Weise verarbeitet werden („Herr der Daten“). Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Kunden erstellt und eingesetzt. Host Europe sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Buch darüber, welche Anlagen durch den Kunden in welchem Umfang genutzt werden. Die Datenverarbeitung erfolgt durch den Kunden. Host Europe hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

2. Fähigkeit der Vertraulichkeit

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

Maßnahmen	RZ Köln (CGN1)	RZ Straßburg (SXB)
Festgelegte Sicherheitsbereiche	X	X
Individuelle Zutrittsberechtigungsvergabe	X	X
Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen	X	X
Dokumentationen von Zutrittsberechtigungen	X	X
Zutrittsdokumentation	X	X
Autorisiertes Wachpersonal - Während der Geschäftszeiten - 24/7 - Sichtkontrollen		X
Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.)	X	X
Besucher-Regulierungen	X	X
Regelmäßige Kontrollgänge durch das Sicherheitspersonal außerhalb des RZ-Bereiches	X	X
Automatisches Zuziehen und Verschließen von Türen	X	X
Schließung aller Gebäudeeingänge, wie Fenster und Türen	X	X

Zusätzliche mechanische Schutzmaßnahmen für das Erdgeschoss oder die Kellerfenster	X	X
Büroräume außerhalb der Arbeitszeit sind verschlossen	X	24/7-Betrieb, daher immer Personal vor Ort
Schutz und Beschränkung der Zutrittswege	X	X
Transponder- oder schlüsselkartenbasierte Schließanlage	X	X
Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes	X	X
Dem im Hauptgebäude 24/7 befindlichen Personal werden die Alarmmeldungen angezeigt	X	
Eingezäuntes Gelände inkl. Videoüberwachung	X	X
Zutrittskontrollsystem mit Chipkarten	X	X
Zusätzliche Zugangsbeschränkung der Serverräume	X	X
Änderung der Standardkennwörter aller System- und Infrastrukturkomponenten	X	X
Protokollierung von Benutzer relevanten Aktivitäten (Anmeldung, Abmeldung, Zugangsverweigerungen, etc.)	X	X
Demilitarisierte Zonen	X	X
Schutz der Infrastruktur durch Einbruchmeldeanlagen	X	X
Zugangsbeschränkungen für bestimmte IP-Adressbereiche	X	X

VPN-Beschränkungen	X	X
Sperrung von nicht erforderlichen Ports	X	X
Externer Zugang nur über sichere Verbindungen (VPN, RDP oder vergleichbar)	X	X
W-LAN-Verschlüsselung	X	X
Regelmäßige Software-Updates	X	X
Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich	X	X
Einschränkung der zeitlichen Gültigkeit der Benutzerkonten	X	X
Automatische Deaktivierung von Benutzern nach mehreren fehlgeschlagenen Logins	X	X
Zwangs- oder Pflicht-Änderung der Kennwörter nach der ersten Anmeldung	X	X
Ablauf von Benutzerpasswörtern	X	X
Erforderliche Mindestkomplexität für Kennwörter	X	X
Passwort-Historie zur Verhinderung der Mehrfachnutzung desselben Passwortes	X	X
Angemessene Gestaltung der Benutzeraccount-Wiederherstellung im Falle eines verlorenen oder vergessenen Authentifizierungsdatensatzes	X	X
Verschlüsselte Speicherung von User-Passwörtern	X	X
User-Login-Verlauf	X	X
Vernichtung von physikalischen Medien nach DIN 66399	X	X

Nutzung eines Aktenvernichters (gem. DIN 66399)	X	X

3. Fähigkeit der Integrität (Gilt für alle RZ-Standorte)

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.

Maßnahmen
Rollenbasiertes Berechtigungskonzept (Lesen / Schreiben / Ändern / Kopieren / Löschen)
Dokumentation der Vergabe von Zugriffsrechten
Strenge administrative Aufgabentrennung
Protokollierung von externen Support-Prozessen
Dokumentation der Weitergabe von physischen Speichermedien
Logische Datentrennung: Separate Datenbanken oder strukturierte Dateiablage
Separate Instanzen für Entwicklungs- und Produktivsysteme (Sandboxes)
Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff / Berechtigungskonzept

4. Fähigkeit der Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Maßnahmen	RZ Köln (CGN1)	RZ Straßburg (SXB)
Schutz der Infrastruktur durch Hardware-Firewalls	X	X
Software-Firewall	X	X
Antivirus-Software auf allen Systemen	X	X
Überwachung und Protokollierung von administrativen Systemzugang und von Konfigurationsänderungen	X	X
Kontrollierter Zugang zu E-Mails und Internet	X	X
Trennung von Anwendungs- und Administrationszugängen	X	X
Überwachung und Protokollierung allgemeiner Benutzeraktivität	X	X
Protokollierung von externen Support-Prozessen	X	X
Protokollierung von administrativen Änderungen	X	X
Zugriffsregelungen und Zugriffsverwaltung	X	X
Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag	X	X
Unterbrechungsfreie-Stromversorgung (USV)	X	X
Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr	X	
Kühlsystem im Rechenzentrum / Serverraum	X	X
Sollte es wider Erwarten zu einer Rauchentwicklung oder gar einem Brand kommen, flutet die aufwendige Feuerbekämpfungsanlage mit 150fachen Luftdruck das Data Center innerhalb von nur 60 Sekunden vollständig mit dem Löschgas Argon.	X	X
Disaster-Recovery-Mechanismen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust	X	X
Tägliche inkrementelle Datensicherung	X	X
Wöchentliche vollständige Datensicherung	X	X
	X	X

Wöchentliche Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen		
Der Kraftstoffvorrat ist für mindestens 16 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich	X	X
Geräte zur Überwachung der Temperatur und Feuchtigkeit in den Data Centern	X	X
Notfallplan	X	X
Externe Audits und Sicherheitstests	X	X
Klar definierte Verwaltungsaufgaben für Auftraggeber und Auftragnehmer	X	X

5. Verfahren zur regelmäßigen Überprüfung (Gilt für alle RZ-Standorte)

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

Maßnahmen
Regelmäßige Überprüfung der Systemzugangsberechtigungen
Interne- und externe Audits
Disziplinarmaßnahmen im Falle einer Datenschutzverletzung
Regelmäßige Sicherheitsprüfungen
Regelmäßige Kontrolle externer Dienstleister
Regelmäßige Besprechungen mit den bestellten Datenschutzbeauftragten in Bezug auf Betriebsprozesse, welche die Verarbeitung von personenbezogenen Daten betreffen

6. Schutz vor unrechtmäßigem Zugang zu personenbezogenen Daten (Gilt für alle RZ-Standorte)

Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

Maßnahmen
Kontrollierter Zugang zu E-Mails und Internet
Trennung von Anwendungs- und Administrationszugängen
Regelmäßige Sicherheits-Updates
Überwachung und Protokollierung allgemeiner Benutzeraktivität
Verbot der Nutzung von privaten Datenträgern
Rollenabhängige Zugriffsbeschränkungen
Applikationsbasierte Überprüfung der Eingabeberechtigung

7. Verarbeitung personenbezogener Daten nur nach Anweisung (Gilt für alle RZ-Standorte)

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

Maßnahmen
Vertraulichkeitserinnerungen
Schriftliche Verpflichtung aller Mitarbeiter auf die Wahrung der Vertraulichkeit
Regelmäßige Datenschutz-Unterweisung der Mitarbeiter
Geregeltes Löschen / Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks
Datentransfer und –weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers
Schriftliche Richtlinien für die Datenübertragung und –weitergabe
Verbindliche Regeln für die Offenlegung von sensiblen Daten
Datenschutzkonforme Löschung aller Datenkopien und Datensicherungen nach Abschluss des Auftrags
Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers
Festgelegte Ansprechpartner für Änderungsanfragen
Kontrollrechte der Auftraggeber bei der Auftragsdatenverarbeitung
Subunternehmer werden auf die gleichen Regelungen und Bestimmungen verpflichtet wie Host Europe selbst

8. Anonymisierung / Pseudonymisierung / Verschlüsselung

Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten des Auftraggebers sind grundsätzlich nicht Gegenstand der von Host Europe zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

9. Belastbarkeit der Systeme

Host Europe unternimmt die unter Ziffer 4 dargestellten Maßnahmen um eine Belastbarkeit der IT-Systeme sicherzustellen. Penetrationstests der IT-Systeme des Auftraggebers sind grundsätzlich nicht Gegenstand der von Host Europe zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.