Anlage
Technische und organisatorische Maßnahmen (Provider-Rechenzentren)

Version: DE – v4.5.6
Stand: 13. April 2021

PlusServer GmbH
Hohenzollernring 72
50672 Köln

Kontakt
Beratung: +49 2203 1045 3500
E-Mail: info@plusserver.com

Sitz
Amtsgericht Köln,
HRB 84977

Umsatzsteuer-ID
DE815289260

Geschäftsführung
Dr. Oliver Mauss
Holger Müller
Dr. Frank Nellissen

Inhaltsverzeichnis

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 einem oder mehreren, 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.

2. Geltungsbereich

Der Geltungsbereich dieses Dokuments erfasst die IT-Systeme der PlusServer GmbH an den nachfolgend genannten Rechenzentrums-Standorten:

Bezeichnung	Rechenzentrumsadresse			
AMS1	Stekkenbergweg 4	1105 AJ	Amsterdam	Niederlande
BER1	Gradestr. 60	12347	Berlin	Deutschland
BRU1	Léon Grosjeanlaan 2	1140	Brüssel-Evere	Belgien
CGN1	Hansestr. 109	51149	Köln	Deutschland
DUS3.2	In der Steele 43	40599	Düsseldorf	Deutschland
DUS4	Alberstr. 27	40233	Düsseldorf	Deutschland
FRA3	Gutleutstr. 310	60327	Frankfurt am Main	Deutschland
FRA4	Lyoner Str. 28	60528	Frankfurt am Main	Deutschland
FRA5	Kleyerstr. 90	60326	Frankfurt am Main	Deutschland
FRA8	Eschborner Landstr. 100	60489	Frankfurt am Main	Deutschland
HAM1	Süderstr. 198	20537	Hamburg	Deutschland
MUC1	Wamslerstr. 8	80335	München	Deutschland
MUC2	Seidlstr. 3	81829	München	Deutschland
NUE1	Thomas-Mann-Str. 16-20	90471	Nürnberg	Deutschland

3. Technische und organisatorische Maßnahmen

3.1. Pseudonymisierung

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der 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, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.

Wir gewährleisten die Pseudonymisierung der Daten wie folgt:

Pseudonymisierung
organisatorisch / technisch
Pseudonymisierung oder Anonymisierung von Daten des Auftraggebers sind grundsätzlich nicht Gegenstand der von PlusServer zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

3.2. Verschlüsselung

Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.

Wir gewährleisten die Verschlüsselung der Daten wie folgt:

Verschlüsselung	
organisatorisch	**technisch**
Passwortrichtlinie und geschützte Passwortvergabe	Authentifizierung mit personifizierten SSH-Keys
-	Einsatz von VPN bei Remote-Zugriffen auf PlusServer-IT-Systeme
	Verschlüsselung von Notebooks / Laptops

3.3. Fähigkeit der Vertraulichkeit

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

Wir gewährleisten die Vertraulichkeit der Daten wie folgt:

Zutritt	
organisatorisch	**technisch**
Personenkontrolle	**Gebäude / Betriebsgelände**
Anwesenheitszeit von Personen im Sicherheitsbereich wird protokolliert	Geschütze Außen-Infrastruktur (z.B. Rückkühler)
Einteilung in Sicherheitszonen / Sperrbereiche	**Meldeanlagen**
Gruppierung der Zutrittsbefugnisse nach Aufgaben- und Zuständigkeitsgebiet	Alarmanlage (z.B. Einbruch-, Kontaktmelder für Zugänge - Fenster, Türen)
Rechte Management	**Kameraüberwachung**
Prozess zur Vergabe/Entzug von Zutrittsrechten und -token	Kameraüberwachung der Gebäudezugänge
Schlüsselregelung (z.B. Universalschlüssel)	Kameraüberwachung der Zugänge zu Rechenzentrumsräumen
Dienstleister Management	**Zutrittsmanagement**
Sorgfältige Auswahl von Personal	2-Faktor-Authentifizierung für den Zutritt zu Rechenzentrumsräumen
Sorgfältige Auswahl von Dienstleistern	-
Zutrittsmanagement	
Zutritt in sensitive Infrastrukturbereiche (NSHV, USV, ...) streng limitiert	
Zutritt in Rechenzentrumsräume streng limitiert	

Zugang	
organisatorisch	**technisch**
Berechtigungskonzept für Zugänge zu PlusServer-IT-Systemen	Authentifizierung mit personifizierten SSH-Keys
Erstellen von Benutzerprofilen	Authentifizierung mit personifizierten Zugangsdaten
Passwortrichtlinie und geschützte Passwortvergabe	Automatische und kennwortgeschützte PC-Bildschirmsperre
Protokollierung von fehlgeschlagene Zugriffsversuche auf PlusServer-Systeme	Einsatz von Anti-Viren-Software auf PlusServer Arbeitsplatzrechnern
Prozess zur Rechtevergabe / zum Rechteentzug	Einsatz von Firewalls zum Schutz der PlusServer-IT-Systeme
Rechtevergabe durch geschultes Personal	Einsatz von VPN bei Remote-Zugriffen auf PlusServer-IT-Systeme
Regelmäßige Überprüfung von Richtlinien auf Aktualität und Wirksamkeit	Verschlüsselung von Notebooks / Laptops
Regelmäßige Überprüfung von Zugangsrechten auf PlusServer-IT-Systeme	-

Zugriff	
organisatorisch	**technisch**
Berechtigungskonzept mit Minimalprinzip etabliert	Berechtigungsebenen nach Abteilungen und Zugriffserfordernissen
Clean-Desk-und Clean-Screen-Richtlinie	Automatische und kennwortgeschützte PC-Bildschirmsperre
Etablierter Datenvernichtungs-/Datenlösch-Prozess	Degausser-Entmagnetisierer für magnetische Festplatten
Etablierter Rechteprozess zur dokumentierten Vergabe/Entzug von Zugriffsrechten	Datenlösch-Systeme zum Löschen mittels DBAN und Secure Erase
Etablierter Rückbauprozess bei Produktkündigungen	Einsatz von Aktenvernichtern oder Entsorgungstonnen
Klassifizierung von Informationen nach vorgegebener Richtlinie	Löschung von Datenträgern vor deren Wiederverwendung
Passwortrichtlinie inkl. Länge, Komplexität und Wechsel	Protokollierung von Zugriffen auf PlusServer Anwendungen und IT-Systeme
Regelmäßige Überprüfung der Richtlinien und Prozesse auf Aktualisierung	Verschlossene Entsorgungstonnen von zertifizierten Datenvernichtern
Sichere Aufbewahrung von Datenträgern	Verschlüsselung von Notebooks/Laptops
Verwaltung der Benutzerrechte durch geschulte Systemadministratoren	-

3.4. Fähigkeit der Integrität

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.

Wir gewährleisten die Integrität der Daten wie folgt:

Fähigkeit der Integrität	
organisatorisch	**technisch**
Berechtigungskonzept mit Minimalprinzip etabliert	Berechtigungsebenen nach Abteilungen und Zugriffserfordernissen
Etablierter Rechteprozess zur dokumentierten Vergabe/Entzug von Zugriffsrechten	Automatische und kennwortgeschützte PC-Bildschirmsperre
Verwaltung der Benutzerrechte durch geschulte Systemadministratoren	Protokollierung von Zugriffen auf PlusServer-Anwendungen und PlusServer-IT-Systeme

3.5. 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.

Wir gewährleisten die Verfügbarkeit der Daten wie folgt:

Fähigkeit der Verfügbarkeit	
organisatorisch	**technisch**
Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	**Brandbekämpfung**
Aufbewahrung von PlusServer-Datensicherungen an einem sicheren, ausgelagerten Ort	Brandmeldeanlage mit Aufschaltung zur Feuerwehr
Monitoring aller relevanten Infrastruktur und IT-Systeme von PlusServer	Feuer- und Rauchmeldeanlagen
-	Feuerlöscher oder Feuerlöschanlage (Argon/Stickstoff) im Serverraum vorhanden
	Feuerlöscher in Büros und Infrastrukturräumen vorhanden
	Klima
	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
	Klimaanlage für Serverräume
	Netzwerk
	Netzwerkanbindung der PlusServer-Core-Router über zwei separate Zuleitungen
	Netzwerkanbindung der PlusServer-Core-Router über mind. zwei unterschiedliche Carrier
	Strom
	Netzersatzanalage vorhanden (Diesel-Aggregat)
	Stromversorgung der Rechenzentrumsräume über zwei Zuleitungen
	Unterbrechungsfreie Stromversorgung - USV-Anlage für Serverräume
	Sonstiges
	Einsatz von Datenspiegelung (RAID) für relevante PlusServer-IT-Systeme

3.6. Fähigkeit der Belastbarkeit

Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

Wir gewährleisten die Belastbarkeit der Daten wie folgt:

Fähigkeit der Belastbarkeit	
organisatorisch	**technisch**
PlusServer unternimmt die unter Ziffer 4.5 („Fähigkeit der Verfügbarkeit“) dargestellten Maßnahmen um eine Belastbarkeit der IT-Systeme unserer Kunden sicherzustellen. Penetrationstests der IT-Systeme des Auftraggebers sind grundsätzlich nicht Gegenstand der von PlusServer zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.	-

3.7. Wiederherstellbarkeit der Verfügbarkeit und des Zugangs

Wir gewährleisten die Wiederherstellbarkeit der Verfügbarkeit und des Zugangs nach Sicherheitsvorfällen wie folgt:

Wiederherstellbarkeit der Verfügbarkeit und des Zugangs	
organisatorisch	**technisch**
Notfallkonzept für relevante Infrastruktur und PlusServer-IT-Systeme vorhanden	-
Testen von Datenwiederherstellung relevanter PlusServer-IT-Systeme	
Maßnahmen gemäß Ziffer 4.5 („Fähigkeit der Verfügbarkeit“)	
Maßnahmen zum Zugang gemäß Ziffer 4.3 („Fähigkeit der Vertraulichkeit“ – Zugang)	

3.8. Verfahren zur regelmäßigen Überprüfung

Wir gewährleisten die regelmäßige Überprüfung der Datensicherungsmaßnahmen wie folgt:

Verfahren zur regelmäßigen Überprüfung	
organisatorisch	**technisch**
Jährliche Überprüfung der Maßnahmen im Rahmen der Wirksamkeitskontrolle	-
Kontinuierlicher Verbesserungsprozess im Rahmen des Informationssicherheitsmanagementsystems (ISMS)	

3.9. Unrechtmäßiger Zugang zu personenbezogenen Daten

Folgende Maßnahmen zur Verhinderung von unrechtmäßigem Zugang zu personenbezogenen Daten sind implementiert:

Unrechtmäßiger Zugang zu personenbezogenen Daten	
organisatorisch	**technisch**
PlusServer unternimmt die unter Ziffer 4.3 („Fähigkeit der Vertraulichkeit“ – Zugang und Zugriff) dargestellten Maßnahmen, um einen unrechtmäßigen Zugang zu personenbezogene Daten zu verhindern.	-

3.10. Verarbeitung personenbezogener Daten nur nach Anweisung

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

Verarbeitung personenbezogener Daten nur nach Anweisung	
organisatorisch	**technisch**
Auftragnehmer hat einen Datenschutzbeauftragten bestellt	-
Regelmäßige Datenschutz-/ und IT-Sicherheits-Schulung der zugriffsberechtigten Mitarbeiter	
Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) gegeben	
Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis	
Weisungen zu Änderungen im Verfahrensablauf erfolgen schriftlich	