Anlage zur Auftragsverarbeitungs-Vereinbarung

Allgemeine Beschreibung der „technischen und organisatorischen Maßnahmen (TOM)“ bei SPECTRUM und eSPECTRUM

gemäß Art. 32 EU-DSGVO

Dieses Beschreibung gilt für die SPECTRUM COMPUTER-SYSTEMHAUS GMBH und/oder die eSPECTRUM Internet-Solution GmbH, beide Max-Planck-Str. 17, 40699 Erkrath gleichermaßen.

Ausgabedatum: April 2026

Inhaltsverzeichnis

Vorwort

Die SPECTRUM COMPUTER-SYSTEMHAUS GMBH (**„SPECTRUM“**) ist ein mittelständisches IT-Systemhaus, welches u.a. auf die Betreuung von IT-Systemen bei Steuerberatern und Wirtschaftsprüfern bzw. deren Mandanten, d.h. Unternehmen spezialisiert ist. Neben klassischen vor Ort IT-Servicearbeiten und Netzwerkbetreuungen beim Auftraggeber hat sich SPECTRUM auf das „Application-Service-Providing“ (ASP) spezialisiert und erbringt „Cloud-Computing“-Leistungen in zwei eigenen Rechenzentren in Düsseldorf und Mönchengladbach. Die eSPECTRUM Internet-Solution GmbH (**„eSPECTRUM“**) ist am gleichen Standort ein Tochterunternehmen für Internet-Dienstleistungen, Providing, Domainverwaltung, WEB-Anwendungen und Softwareentwicklung.

SPECTRUM und eSPECTRUM nutzen in Teilbereichen gemeinsam ein Rechenzentrum und Auftraggeber nutzen zum Teil Leistungen beider Auftragnehmer (d.h. von SPECTRUM bzw. eSPECTRUM).

Aus diesem Grunde gelten diese technisch-organisatorischen Maßnahmen hier für SPECTRUM und eSPECTRUM.

Mit-Nutzung eines CoLocation-Rechenzentrums:

Das SPECTRUM-/eSPECTRUM-eigene Rechenzentrum setzt auf der Basis-Infrastruktur eines großen CoLocation-RZ-Betreibers in Düsseldorf auf.

Diese von SPECTRUM/eSPECTRUM eingekaufte bzw. angemietete CoLocation-Infrastruktur (WIIT AG, Joachim-Erwin-Platz 3, 40212 Düsseldorf) beinhaltet folgende Leistungen im RZ:

- Zutritts- und Zugangskontrolle,
- 24/7 Objektschutz durch einen externen Sicherheitsdienst,
- Alarmanlage und 24/7h-Video-Überwachung,
- zweifache, ringförmige Anbindung an das öffentliche 10 KV-Netz
- mit eigener Niederspannungsversorgung,
- mit eigenem Blockkraftwerksbetrieb,
- mit unterbrechungsfreier Stromversorgung (USV),
- mit Dieselgenerator-Notstrombetrieb (Tier III+),
- mit voll redundant ausgelegter Klimaanlage,
- mit Brandmeldeüberwachung und Argon-Gas-Löschanlage,
- mit Multi-Carrier-Hochgeschwindigkeits-Internet-Anbindung
- mit 24/7 Routing-Überwachung und Administration,
- mit aufgeteilter RZ-Fläche in mehrere Brandabschnitte usw..

WIIT THE PREMIUM CLOUD

Zertifikat
Geprüftes Rechenzentrumsmanagement nach ISO 27001
TÜV SAARLAND Geprüftes Rechenzentrums-management nach ISO 27001

SPECTRUM und eSPECTRUM haben dort zusammen einen eigenen, abgesicherten, abgetrennten und exklusiven Bereich („Cage“) angemietet. Es bestehen mit dem CoLocation-RZ-Betreiber 24/7-Wartungsverträge mit entspr. Service-Level-Agreements („SLA“), Vereinbarungen über die einzuhaltenden „technischen und organisatorischen Maßnahmen (TOM)“ und eine „Vereinbarung zur Auftragsverarbeitung nach Art. 28 der EU-DSGVO“.

Die „**Leistungsbeschreibung dieses CoLocation-Rechenzentrums“**, die **„Spezifikation der Service-Level-Agreements (SLA)“**, die **„technisch-organisatorischen Maßnahmen (TOM)“** und die **ISO-27001-Zertifizierung** dieses CoLocations-RZ-Betreibers können jeweils aktuell unter „Leistungsbeschreibung des von SPECTRUM und eSPECTRUM genutzten CoLocation-Rechenzentrums (nachfolgend „SPECTRUM-RZ“ genannt) unter www.spectrum-kundenbereich.de eingesehen werden.

Für SPECTRUM und eSPECTRUM sind, sowohl als Auftragnehmer als auch als Auftragsverarbeiter, der Datenschutz von besonderer Bedeutung. Daher haben SPECTRUM und eSPECTRUM Schutzmaßnahmen für jeglichen Umgang mit vertraulichen oder sicherungsbedürftigen Daten etabliert, die im Rahmen des technischen Fortschritts stetig weiterentwickelt werden.

Die grundlegende Verpflichtung zum Schutz personenbezogener Daten im Rahmen der Verarbeitung konkretisiert Art. 32 EU-DSGVO, der besondere Anforderungen an die Sicherheit der Verarbeitung stellt. Der Verantwortliche hat ein den festgestellten Risiken angemessenes Schutzniveau sicherzustellen. Zu verhindern ist insbesondere, dass personenbezogene Daten unbeabsichtigt und/oder unrechtmäßig vernichtet, verändert oder unbefugt offengelegt werden oder auf sonstige Weise verloren gehen bzw. Dritte unbefugt Zugang zu verarbeiteten personenbezogenen Daten erhalten.

Gesetzesgrundlage

Hier zunächst nachfolgend einige Grundlagen aus der europäischen Datenschutz-Grundverordnung (EU-DSGVO) zum besseren Verständnis:

Art. 30 EU-DSGVO „Verzeichnis von Verarbeitungstätigkeiten“:

a) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgende Angaben:
   (1) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
   (2) die Zwecke der Verarbeitung;
   (3) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
   (4) die Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
   (5) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 EU-DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
   (6) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
   (7) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 EU-DSGVO.

b) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:
   (1) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
   (2) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
   (3) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
   (4) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 EU-DSGVO.

Art. 32 Abs. 1 EU-DSGVO „Sicherheit der Verarbeitung“:

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 Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

„Technische und organisatorischen Maßnahmen (TOM)“

Nachfolgend befindet sich die Beschreibung der „technischen und organisatorischen Maßnahmen (TOM)“ der SPECTRUM COMPUTER-SYSTEMHAUS GMBH („SPECTRUM“) und der eSPECTRUM Internet-Solution GmbH (eSPECTRUM“) beide am Standort Max-Planck-Str. 17, 40699 Erkrath gemäß Art. 32 Abs. 1 EU-DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. a) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. b) inkl. der Einwahltechnik auf das SPECTRUM-RZ:

Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen behält sich SPECTRUM bzw. eSPECTRUM vor, sofern das Schutzniveau nach EU-DSGVO nicht unterschritten wird.

I. Pseudonymisierung

Grundsätzlich können Daten mit einem Pseudonym, d.h. einem nicht personenbezogenen Namen, einer Nummer oder Ähnlichem versehen werden, welches eine Zuordnung erschwert. Wichtig für eine wirksame Pseudonymisierung ist dabei, dass die pseudonymisierten Daten ohne Hinzuziehung zusätzlicher Informationen keine Zuordnung erlauben. Als Auftragsverarbeiter trifft SPECTRUM bzw. eSPECTRUM keine Maßnahmen zur Pseudonymisierung, es sei denn, dass der Auftraggeber SPECTRUM bzw. eSPECTRUM hierzu beauftragt oder wenn sich eine Pseudonymisierung aus den jeweiligen Leistungsbeschreibungen der Produkte / Dienstleistungen von SPECTRUM oder eSPECTRUM ergibt.

II. Verschlüsselung

Daten können verschlüsselt werden. Hierbei wird die Information mit Hilfe eines kryptografischen Verfahrens in eine nicht lesbare Zeichenfolge verwandelt. Bei der Nutzung der Verschlüsselung bleibt der Personenbezug der Daten erhalten. Die Daten werden jedoch auf Basis von mathematischen Algorithmen so verändert, dass sie ohne Kenntnis des zugehörigen Schlüssels mit der aktuell verfügbaren Technik nicht lesbar gemacht werden können.

Zur Verschlüsselung setzen SPECTRUM und eSPECTRUM für den elektronischen Transport Verschlüsselungsverfahren ein, die dem Stand der Technik entsprechen und ein Schutzniveau erreichen, das den Anforderungen z.B. von Berufsgeheimnisträgern (wie Steuerberatern, Wirtschaftsprüfern, Rechtsanwälten, Ärzten usw.) angemessen ist.

Dies sind für den elektronischen Transport zwischen Rechenzentrum

- und dem Verantwortlichem: über VPN- oder TLS-Verbindung mit Zertifikaten oder Zwei-Faktor-Authentifikation abgesichert
- und Einzelpersonen: abgesichert mit Verschlüsselungsverfahren nach dem Stand der Technik
- und Mitarbeitern von SPECTRUM: Verschlüsselte Verbindung mit Zertifikaten oder Zwei-Faktor-Authentifikation.

Mobile Endgeräte der SPECTRUM- bzw. eSPECTRUM-Mitarbeiter (SmartPhone, Tablet, Notebook) werden – sofern hier personenbezogene Daten verarbeitet werden - verschlüsselt und mit Passwort geschützt.

III. Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

Maßnahmen sollen die Vertraulichkeit der verwendeten Systeme & Dienste schützen. Es soll verhindert werden, dass es zu unbefugter oder unrechtmäßiger Verarbeitung kommt. Hierunter fallen Maßnahmen, welche den Zutritt, Zugang und Zugriff auf Systeme und Dienste regeln (Beispiele: Bauliche Maßnahmen, Zugangskontrollen, Zugriffsrechte, Alarmanlagen). Ebenso soll die Integrität der Systeme geschützt werden. Daten sollen stets richtig und verlässlich sein und dürfen nicht unbeabsichtigt oder schadhaft geändert oder zerstört werden können.

a) Vertraulichkeit

Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Die Vertraulichkeit von Systemen (Hardware) und Diensten (Software) setzt im Rahmen der Verarbeitung zwingend ein Zugriffskonzept voraus, das mit Gruppen- und Benutzerrechten arbeitet und den Zugriff auf einzelne Daten im Rahmen der Verarbeitung abhängig von den erforderlichen Prozessen ermöglicht. Hierzu gehören auch Maßnahmen der Zutrittskontrolle, der Zugangskontrolle und der Zugriffskontrolle.

Alle im Auftrag verarbeiteten Daten des Auftraggebers werden grundsätzlich im SPECTRUM-Rechenzentrum gespeichert, der als getrennter Sicherheitsbereich ausgelegt ist. Siehe „Leistungsbeschreibung des von SPECTRUM und eSPECTRUM genutzten CoLocation-Rechenzentrums WIIT in Düsseldorf“ unter www.spectrum-kundenbereich.de.

1. Benutzer-/Rechteverwaltung - Authentifizierung

SPECTRUM bzw. eSPECTRUM hat für am IT-System zugelassene Benutzer und angelegte Benutzergruppen Rechteprofile erstellt. In Anlehnung an die Maßnahme M 2.31 des BSI IT-Grundschutz (Dokumentation der zugelassenen Benutzer und Rechteprofile) umfasst dies folgende Angaben:

(1) Rechtevergabe an zugelassene Benutzer
- zugeordnetes Rechteprofil (in Einzelfall mit Abweichungen vom verwendeten Standard-Rechteprofil)
- Begründung für die Wahl des Rechteprofils und gegebenenfalls der Abweichungen
- Zuordnung des Benutzers zu einer Organisationeinheit mit Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung / Löschen der Benutzergruppen

(2) Rechtevergabe an zugelassene Gruppen
- zugehörige Benutzer
- Zeitpunkt der Einrichtung
- Befristung der Einrichtung

2. Zutrittskontrolle

- Das Gebäude (Standort des SPECTRUM- und eSPECTRUM-Firmensitzes Max-Planck-Str. 17, 40699 Erkrath) ist 24/7 verschlossen, SPECTRUM-Mitarbeiter haben einen Token (Chip) zum Öffnen des elektronisch gesicherten Hauseinganges. Fremde müssen sich per Sprechanlage anmelden und erhalten dann eine elektronische Türfreischaltung, um das Gebäude betreten zu können.
- Die Räume von SPECTRUM und eSPECTRUM befinden sich in der ersten Etage und sind durch eine Sicherheitstüre vom restlichen Gebäude getrennt.
- Die SPECTRUM-/eSPECTRUM-Büroetage ist durch eine Alarmanlage, die an einen Wachdienst aufgeschaltet ist, gesichert.
- In der SPECTRUM-/eSPECTRUM-Büroetage erfolgt eine Videoüberwachung für den Eingangsbereich sowie für Flure, Serverräume und den kompletten Werkstattbereich.
- Der Empfangsbereich bei SPECTRUM ist wochentags durchgehend von 09.00 Uhr – 18.00 Uhr besetzt.
- Alle Personen müssen sich am Empfang anmelden. Vor Einlassgewährung wird Rücksprache mit dem Besuchten gehalten. Der Besucher wird am Empfang abgeholt und wird stets von einem SPECTRUM-/eSPECTRUM-Mitarbeiter begleitet.
- Das Grundstück (Max-Planck-Str. 17, 40699 Erkrath) ist eingezäunt und nachts (20:00 – 6:00 Uhr) außerdem mit einer elektronischen Torschließanlage verschlossen.
- Zusätzlich sind im gesamten Gebäude für die Büroetagen Sicherheitsschlösser verbaut. Die Schlüsselvergabe ist strikt geregelt und dokumentiert. Schlüssel werden nur an SPECTRUM- und eSPECTRUM-Mitarbeiter vergeben, die auf den Datenschutz verpflichtet sind. Dritte erhalten keine Schlüssel.
- Außerhalb der Arbeitszeiten sind die Gebäude-Innentüren per Sicherheitsschlüssel verschlossen.

- Die Einwahltechnik auf das SPECTRUM- und eSPECTRUM-Rechenzentrum in Düsseldorf befindet sich in einem abgetrennten Raum der Büroetage mit Sicherheitscode.
- Der Zutritt zum SPECTRUM-/eSPECTRUM-Rechenzentrum ist nur speziell autorisierten Mitarbeitern von SPECTRUM und eSPECTRUM gestattet.
- Die Geschäftsleitung von SPECTRUM und eSPECTRUM prüfen periodisch die Notwendigkeit von Zutrittsberechtigungen der Mitarbeiter.

3. Zugangskontrolle

(1) Zunächst greifen alle Maßnahmen der voran beschriebenen Zutrittskontrolle.

(2) Alle Rechner (Arbeitsplatz-PC's, Server, Tablets, SmartPhones usw.) bei SPECTRUM und eSPECTRUM verfügen mindestens über ein Zugangskontrollsystem (UserID, Passwort). Es gibt vorgeschriebene Regeln zur Passwortvergabe. Dies betrifft die notwendige Komplexität, die Lebensdauer des Passwortes sowie die Wiederverwendung alter Passwörter.

(3) Zur Prüfung der Wirksamkeit der Absicherungsmaßnahmen werden bei sensiblen Systemen in Zeitabständen Penetrationen durchgeführt.

(4) Arbeitsplatz-PC-Sicherheit:
- Benutzerkennung mit mindestens 8-stelliger Passwortvergabe. Jeder User bekommt eine eigene Benutzerkennung mit eigenem Passwort. (Netzwerk Authentifizierung).
- Automatische passwortgeschützte Bildschirm- und PC-Sperren.
- Alle Mitarbeiter von SPECTRUM und eSPECTRUM werden kontinuierlich angewiesen, ihre PC's bei kurzzeitigem Verlassen des Arbeitsplatzes zu sperren. Die Einhaltung dieser Anweisung wird strengstens überwacht.
- Für alle Remote-Zugänge bei SPECTRUM und eSPECTRUM geschieht der Zugang grundsätzlich mit einer 2-Faktor-Autorisierung.

(5) Zugangskontrolle zu Systemen zur Auftragsbearbeitung:
- Die zur Benutzung von IT-Systemen Berechtigten dürfen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen.
- Im Auftrag verarbeitete Daten dürfen bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.
- Die eingesetzten IT-Systeme haben ein dediziertes Rechtesystem, welche es ermöglicht, Datenzugriffe und -veränderungen auf Basis von Rollen und individuellen Berechtigungen zu vergeben.
- Es gibt vorgeschriebene Regeln zur Passwortvergabe.

4. Zugriffskontrolle

- Innerhalb des hausinternen SPECTRUM-und eSPECTRUM-Firmennetzwerks werden für verschiedene User unterschiedliche Berechtigungsrollen vergeben. So wird gewährleistet, dass ein Nutzer nur auf solche Verzeichnisse oder Bereiche Berechtigungen erhält, die er auch sehen darf.
- Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen.
- Zusätzlich ist das SPECTRUM- und eSPECTRUM-Firmennetzwerk in differenzierte hausinterne Netzsegmente eingeteilt. User können folglich nicht auf bestimmte Server zugreifen.

5. Zugriff auf das Rechenzentrum:
- Der Zugriff erfolgt nur über VPN-Verbindungen oder über SPECTRUM-/eSPECTRUM-eigene Punkt-zu-Punkt-Glasfaserstrecken.
- Die Datenübertragung zwischen SPECTRUM, eSPECTRUM und den lokalen Netzen der Auftragnehmer oder anderen Kommunikationspartnern erfolgt grundsätzlich

verschlüsselt. Unter der „Leistungsbeschreibung SPECTRUM-NET-Gateway“ unter www.spectrum-kundenbereich.de befindet sich die Beschreibung für diese VPN-Verbindung.

- Auf die Server der Auftraggeber im SPECTRUM-Rechenzentrum, im Rahmen der Auftragsverarbeitung, kann von den SPECTRUM- und eSPECTRUM-Mitarbeitern über das SPECTRUM-Firmennetzwerk nicht direkt zugegriffen werden. Hier erfolgt der Zugriff immer über eine dazwischengeschaltete Sicherheits-Ebene (Admin-Server). Hier werden auch alle Zugriffe kontinuierlich protokolliert und die Zugriffe von der SPECTRUM- und eSPECTRUM-Geschäftsleitung turnusmäßig stichprobenartig anhand der erteilten Auftragsverarbeitungs-Aufträge und den Einträgen im Ticket-System überprüft.
- Die IT-Systeme von SPECTRUM und eSPECTRUM werden kontinuierlich auf die Wirksamkeit eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter getestet.

6. Sicherheitsmaßnahmen bei Fernwartung

- Der Aufbau der Fernwartungsverbindung darf nur durch den Auftraggeber erfolgen; Fernwartungsarbeiten dürfen nur mit seiner Zustimmung begonnen werden.
- SPECTRUM bzw. eSPECTRUM protokollieren die Fernwartungsaktivitäten mit Datum, Uhrzeit und Benutzerkennung automatisch.
- SPECTRUM bzw. eSPECTRUM darf von den eingeräumten Zugriffsrechten nur in dem für die Durchführung der Fernwartungsarbeiten unerlässlich notwendigen Umfang Gebrauch machen.
- SPECTRUM bzw. eSPECTRUM darf personenbezogene Daten nur dann vom DV-System des Auftraggebers herunterladen und auf den eigenen Systemen speichern, wenn zuvor die Erlaubnis des Auftraggebers in Textform vorliegt.
- Der Auftraggeber ist berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.
- SPECTRUM bzw. eSPECTRUM müssen personenbezogene Daten, die bei der Fernwartung übermittelt wurden, unverzüglich löschen oder dem Auftraggeber zurückgeben, wenn sie für die Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind.

b) Integrität

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren. Die Integrität ist neben der Verfügbarkeit und Vertraulichkeit eines der drei klassischen Ziele der Informationstechnologie. Die Integrität von Systemen und Diensten erfordert die Absicherung gegen Manipulationen.

Dazu zählen:

- die Wahrung der referentiellen Sicherheit in Datenbanken
- die Protokollierung von Änderungen
- das Durchführen von Plausibilitätsprüfungen
- die Verhinderung der Eingabe von ungültigen Werten
- die Verhinderung der ungewollten Löschung, Überschreibung oder Änderung von Daten

Es ist sicherzustellen, dass Programme und Daten nicht verfälscht und/oder falsche Daten verarbeitet werden, damit sie nicht unbemerkt fehlerhafte Ergebnisse erzeugen oder Funktionen ausführen, die nicht erwünscht sind.

SPECTRUM und eSPECTRUM haben mit den Herstellern der eingesetzten Komponenten im Rechenzentrum, mit dem CoLocation-RZ-Betreiber und den Internet-Anbindungs-Providern grundsätzlich Service-Level-Agreements (SLA) geschlossen. Hierbei werden von den Herstellern/Providern SPECTRUM bzw. eSPECTRUM laufend bekannte Schwachstellen gemeldet, um geeignete Maßnahmen zur Risikoreduzierung und Fehlerbehebung zu treffen.

Die persönliche Verantwortung jedes SPECTRUM- und eSPECTRUM-Mitarbeiters für die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen wird bei SPECTRUM und eSPECTRUM durch jährliche Schulungsmaßnahmen, weitergehende Seminare und zentral bereitgestellte Informationen gestärkt.

In den Sicherheitsbereichen des SPECTRUM-RZs gilt ein grundsätzliches Fotografierverbot. Das Verbot ist für alle Benutzer des CoLocation-Rechenzentrums verbindlich geregelt, es wird von den Führungskräften und vom Sicherheitsdienst überwacht.

Für den Sicherheitsbereich des SPECTRUM-RZs haben nur wenige, besonders autorisierte Mitarbeiter Zutritt. Jeder Zutritt wird protokolliert.

1. Weitergabekontrolle

SPECTRUM bzw. eSPECTRUM stellt sicher, dass personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Hierzu wählt SPECTRUM bzw. eSPECTRUM geeignete Maßnahmen wie Verschlüsselung o.ä. bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger.

Sicherung bei der elektronischen Übertragung:

- Bei der elektronischen Übertragung von Auftragnehmerdaten in das SPECTRUM-RZ sind alle Verbindungen über einen VPN-Tunnel verschlüsselt.
- Die elektronische Übertragung von Auftragnehmerdaten in das SPECTRUM-RZ wird protokolliert.
- Bevor die elektronische Übertragung stattfindet, wird geprüft, ob diese zulässig ist.

Sicherung bei der Lagerung und Transport:

- Es besteht ausreichender Zugriffsschutz zwischen dem Speichern der Daten auf den Datenträgern und dem Transport. Die Datenträger liegen in Erkrath in einem gesicherten Raum und dort in Datensicherungsschränken, die nur Mitarbeitern mit einer entsprechenden Berechtigung zugänglich sind.
- Der Transport von Sicherungsdatenträgern wird ausschließlich durch eigene SPECTRUM- bzw. eSPECTRUM-Mitarbeiter in verschlossenen speziellen Transportboxen durchgeführt. Der Transport bzw. Transportweg wird in einem Protokoll festgehalten.
- Alle Datenexporte verlassen das Unternehmen nur verschlüsselt.
- Datenexporte werden durch das Vier-Augen-Prinzip geprüft

2. Eingabekontrolle

Maßnahmen zur Gewährleistung der nachträglichen Überprüfung und Nachvollziehbarkeit der Datenverwaltung und -pflege, insbesondere hinsichtlich Eingabe, Veränderung oder Löschung von Daten.

- Scannen von Dokumenten:
  - Im Scanprozess wird protokolliert, welcher Mitarbeiter ein Dokument bearbeitet hat.
  - Alle Dokumente werden revisionssicher in einem Dokumentenmanagementsystem (DMS) archiviert.
  - Alle Vorgänge werden protokolliert. Protokolle werden stichpunktartig ausgewertet.
- Erfassung von Kundendaten:
  - SPECTRUM bzw. eSPECTRUM erfassen nur Kundendaten, die auftragsrelevant sind.

3. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten lediglich entsprechend den Weisungen des jeweiligen Auftraggebers verarbeitet werden.

SPECTRUM und eSPECTRUM haben hierzu die folgenden Maßnahmen festgelegt:

- Schriftliche Vereinbarungen und Verträge
- Klare Abgrenzung der Kompetenzen und Pflichten zwischen SPECTRUM, eSPECTRUM und Auftraggeber
- Festlegung der Sicherheitsmaßnahmen
- Weisungsbefugnisse eindeutig definiert
- Vor-Ort-Kontrollen
- Vereinbarungen zur Auftragsverarbeitung nach Art. 28 der EU-DSGVO

4. Trennungskontrolle

Es ist sicher zu stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.

Stichpunktartig hier die wichtigsten Maßnahmen, die SPECTRUM und eSPECTRUM umgesetzt haben:

- Trennung von Produktiv- und Test-System
- Getrennte Ordnerstrukturen (Mandantenfähigkeit)
- Getrennte Tables in der Datenbank
- Getrennte Datenbanken
- Getrennte Server

5. Löschen von Daten

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es die Zwecke, für die sie verarbeitet werden, erforderlich machen. Die Leistungsbeschreibungen von SPECTRUM bzw. eSPECTRUM für Produkte und Dienstleistungen – einsehbar unter www.spectrum-kundenbereich.de – die Kundenaufträge (Auftragsbestätigungen von SPECTRUM und eSPECTRUM) und die Vereinbarungen zur Auftragsverarbeitung nach Art. 28 der EU-DSGVO mit den Auftraggebern sehen hier verschiedene Löschkonzepte vor.

- Vernichtung von Datenträgern:
  Datenträger werden zentral in eigens hierfür vorgehaltene verschlossene spezielle Behälter bei SPECTRUM/eSPECTRUM zwischengelagert und nach spätestens 6 Monaten nach DIN-66399 („Büro- und Datentechnik – Vernichtung von Datenträgern Teil 3: Prozess der Datenträgervernichtung, Februar 2013" nach Schutzklasse 3 und Sicherheitsstufe 4) von einem externen Entsorger Datenschutz-konform vernichtet, mit dem SPECTRUM/eSPECTRUM eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 EU-DSGVO hat.

- Vernichtung von Schriftstücken:
  Papierbezogene Akten werden ebenfalls in speziellen Containern zwischengelagert und nach DIN-66399 bzw. DIN-EN-15713 zertifiziert von einem externen Entsorger vernichtet, mit dem SPECTRUM eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 EU-DSGVO hat.

Die Löschung von Kundendaten auf ASP-, IaaS- und Server-Housing-Systemen oder bei Cloud-Speicher-Lösungen (wie SPECTRUM-WEB-Tresor, SPECTRUM-ePendelordner, SPECRUM-RMS usw.) liegt in der Verantwortung der Auftraggeber und wird von SPECTRUM bzw. eSPECTRUM nur nach ausdrücklicher schriftlicher Weisung durchgeführt. Die Aufbewahrungsfristen der Daten werden im Rahmen der vertraglichen Beauftragung durch den Kunden vorgegeben bzw. ergeben sich aus den gesetzlichen Aufbewahrungsfristen.

6. Mandantentrennung

Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet. Daten von Auftraggebern werden im Rahmen der Auftragsverarbeitung getrennt verarbeitet, verwaltet und logisch getrennt.

7. Protokollierung

Die Verarbeitung von im Auftrag verarbeiteten Daten werden grundsätzlich protokolliert und der Verantwortliche (Auftraggeber) erhält jeweils umgehend nach jeder Tätigkeit per E-Mail eine Beschreibung der durchgeführten Arbeiten in Form eines Servicescheins.

Die Dateneingabe und die Verarbeitung der im Auftrag verarbeiteten Daten erfolgen ausschließlich nach dem mit dem Auftraggeber festgelegten Verfahren.

c) Verfügbarkeit

Das Glossar des IT-Grundschutzkataloges des BSI definiert Verfügbarkeit wie folgt:

> *„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.“*

Gemeint ist damit die jederzeitige Betriebsbereitschaft von Systemen und Diensten im Sinne der Sicherstellung einer jederzeitigen Nutzbarkeit.

SPECTRUM und eSPECTRUM stellen sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

Alle Alarmierungspläne, Handlungsanweisungen, Notfallregelungen sowie Wiederanlaufpläne sind in einem elektronischen Notfallhandbuch festgehalten. SPECTRUM und eSPECTRUM führen eine laufende Überwachung der Nutzung der Dienste und der Auslastung der Systeme durch. SPECTRUM und eSPECTRUM haben ein Notfallkonzept umgesetzt, das z. B. Maßnahmen zur Abwehr von Angriffen aus dem Internet beinhaltet. Dieses Notfallkonzept wird laufend fortgeschrieben und regelmäßig auf Wirksamkeit geprüft.

- Für die IT-Infrastruktur am SPECTRUM-/eSPECTRUM-Standort (Max-Planck-Str. 17, 40699 Erkrath) sind hier einige wesentlichen Maßnahmen stichpunktartig genannt:
  - Klimaanlagen im Serverraum
  - Unterbrechungsfreie Stromversorgung (USV)
  - Zugangskonzept für das Gebäude
  - Mehrstufiges Backupkonzept
  - RAID Verfahren
  - Datenübertragung und Datenspiegelung
  - Cluster-Betrieb und redundante Systeme
  - Alle Server werden live überwacht.
- Für die IT-Infrastruktur im SPECTRUM-RZ in Düsseldorf sind folgende wichtige Maßnahmen stichpunktartig genannt:
  - Die Server- und Storage-Systeme, die Einwahl- und Router-Technik, die Switche und Internet-Anbindungen im SPECTRUM-RZ sind doppelt, gespiegelt, geclustert oder anderweitig redundant bzw. ausfallgesichert aufgebaut.
  - SPECTRUM und eSPECTRUM halten Ersatzteile und Ersatzgeräte vor bzw. haben mit Herstellern Subcontractor-Wartungsverträge mit entsprechenden Service-Level-Agreements (SLA) und kurzen Reaktionszeiten, um bei einem Komponentenausfall umgehend einen Not- bzw. Ersatzbetrieb sicherstellen zu können, der geeignet ist, die Rechenzentrumsleistungen grundsätzlich aufrecht zu erhalten.
  - Wartungen der Hardware sind Bestandteil der SPECTRUM- bzw. eSPECTRUM-Grundleistungen bei Server-Housing-, IaaS- und ASP-Verträgen.
  - Regelmäßige Wartungen gewährleisten die Betriebsbereitschaft, die Leistungsfähigkeit sowie das Qualitätsniveau der Systeme.

- Das Einspielen von Patches und Hotfixes erfolgt regelmäßig, sobald diese verfügbar sind und nach SPECTRUM-/eSPECTRUM-internen Tests freigegeben wurden.
- Die Server- und Storage-Systeme im SPECTRUM-RZ werden durch den Einsatz von Managed-Service-Softwareagenten permanent überwacht.
- Das Monitoring und das Management der gesamten RZ-Systemlandschaft trägt zum Erhalt der Betriebsbereitschaft sowie der Leistungsfähigkeit der Systeme bei.

Zweckbindung:

- Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Dies gilt insbesondere auch für die Löschung von Daten.
- Die Verarbeitung von Auftragsdaten erfolgt ausschließlich entsprechend den produktbezogen Leistungsbeschreibungen bzw. den individuellen Vereinbarungen mit dem Auftraggeber.
- Individuelle Weisungen oder Auskunftsersuchen des Auftraggebers werden nur nach einer verifizierbaren Authentisierung (auch E-Mail) im Rahmen des vereinbarten Leistungsumfangs angenommen.
- Weisungen zur Verarbeitung und insbesondere zur Löschung von im Auftrag verarbeiteten Daten werden nur ausgeführt, wenn der Auftraggeber sie in der vertraglich vorgeschriebenen Form erteilt. Dies gilt besonders für die Neuanlage, das Ändern oder die Deaktivierung von Benutzern und deren Zugriffsrechten auf ein Server-Housing-, IaaS- oder ASP-System von SPECTRUM/eSPECTRUM.

d) Belastbarkeit

Die Belastbarkeit umfasst u.a., dass Systeme ausreichend dimensioniert sind, um Verarbeitungen ohne Ausfälle und Wartezeiten durchführen zu können. Ebenso ist hiermit die Toleranz eines Systems gegenüber Störungen gemeint, die in der IT allgemein als „Resilienz“ beschrieben wird („Resilienz“ = die Fähigkeit von technischen Systemen, bei Störungen bzw. Teil-Ausfällen nicht vollständig zu versagen, sondern wesentliche Systemdienstleistungen aufrecht zu erhalten). Dies umfasst auch die Ausfallsicherheit der IT-Systeme und Dienste.

Die für unternehmenskritische Prozesse eingesetzten IT-Systeme sind hochredundant ausgelegt. SPECTRUM und eSPECTRUM verfügen über eine skalierbare IT-Architektur, die eine schnelle und flexible Reaktion auf die Veränderung der Bedingungen durch Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall sicherstellt.

An dieser Stelle sei auch auf den Notfallplan der SPECTRUM bzw. eSPECTRUM verwiesen. Sämtliche Maßnahmen werden durch permanentes Monitoring überwacht und dokumentiert. Zusätzlich prüfen SPECTRUM und eSPECTRUM durch regelmäßige Wiederanlauf-Tests die ordentliche Funktionsweise aller getroffenen Maßnahmen.

Für ASP-, IaaS- und Server-Housing-Leistungen weist SPECTRUM/eSPECTRUM hier auf die entspr. Leistungsbeschreibungen und Geschäftsbedingungen unter www.spectrum-kundenbereich.de hin. Hier finden sich unter dem Punkt „Verfügbarkeit - Service-Level-Agreements (SLA) und Schadensersatzregelung“ detaillierte Ausführungen zur Belastbarkeit von Rechenzentrums-Leistungen.

Für die Anbindung von lokalen Kunden-Netzwerken an das Internet bietet SPECTRUM bzw. eSPECTRUM den abgesicherten Internet-Zugang SPECTRUM-NET an. In SPECTRUM-NET sorgt eine Vielzahl von Mechanismen für die Absicherung gegen Gefahren aus dem Internet (z.B. Proxy-Systeme, Firewalls, Viren-Scanner, Filter-Systeme usw.). Unter www.spectrum-kundenbereich.de „Leistungsbeschreibung SPECTRUM-NET, der abgesicherte Internet Zugang“ finden Sie weitere Informationen hierzu.

IV. Wiederherstellbarkeit

Als weitere technische Maßnahme beschreibt Art. 32 Abs. 1 lit. c) DSGVO die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall ist zu reduzieren.

SPECTRUM und eSPECTRUM haben hierzu u.a. folgende Maßnahmen etabliert:

- Sicherung der Installationen (Bare-Metal-Recovery)
- Sicherung der Daten
- Sicherung von Systemdateien und Datencontainern
- Sicherung von LOG-Dateien
- Sicherung von Benutzerkonten

Siehe hierzu auch „Leistungsbeschreibung Datensicherung im SPECTRUM-RZ bei Server-Housing-, IaaS- und ASP-Leistungen“ unter www.spectrum-kundenbereich.de.

V. Organisatorische Maßnahmen

Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen und zur Gewährleistung der Sicherheit der Verarbeitung bei SPECTRUM und eSPECTRUM etabliert. Der externe Datenschutzbeauftrage hat sich bei seiner Unternehmensdatenschutzanalyse von den oben beschriebenen Maßnahmen überzeugt. Im Zuge der Umstellung auf die EU-DSGVO wird ein regelmäßiges Datenschutzaudit durch den Datenschutzbeauftragten durchgeführt und dokumentiert.

Die Einsicht der Protokolle der Hard- und Software-Komponenten der Infrastruktur gehört zu den täglichen Aufgaben des zuständigen IT-Administrators. Darüber hinaus ist ein System der Benachrichtigung bzw. Alarmierung bei automatisierten Vorgängen eingerichtet.

SPECTRUM hat ein Qualitäts-Managementsystem nach DIN ISO 9001:2015 für den Geltungsbereich „Beratung, Vertrieb, Installation, Einführung und Betreuung von komplexen IT-Systemen mit eigenem Hochsicherheits-Rechenzentrum“ implementiert und zertifizieren lassen. Durch regelmäßige interne Audits wird die Wirksamkeit der getroffenen Maßnahmen geprüft, um ggf. Maßnahmen weiterzuentwickeln. Zur Aufrechterhaltung des Zertifikats werden regelmäßige Re-Zertifizierungsaudits durchgeführt.

Deutsche Qualitätsmanagement Akademie GmbH
www.dqm-akademie.de

Zertifikat

Hiermit wird bescheinigt, dass das Qualitätsmanagement-System der

SPECTRUM
COMPUTER - SYSTEMHAUS GMBH

SPECTRUM COMPUTER-SYSTEMHAUS GMBH
DE - 40699 Erkrath - Max-Planck-Str. 17

geprüft und bewertet wurde
sowie durch den Audit-Bericht Nr. 070.3/53/25
den Nachweis erbracht hat, dass die Forderungen der

DIN EN ISO 9001:2015

für den Anwendungsbereich

Beratung, Vertrieb, Installation, Einführung und Betreuung von komplexen IT-Systemen mit eigenem Hochsicherheits-Rechenzentrum

erfüllt sind.

Dieses Zertifikat mit Nr. 0134/26 ist gültig bis 31.12.2028.

Lead-Auditor/EFQM-Assessor

Internes Audit Regelwerk RW 011:19

www.isocert.de

Zertifikat

Prüfungsnorm **ISO/IEC 27001:2022**

Zertifikat-Registrier-Nr. **01 153 2400138**

Unternehmen:

WIIT
THE PREMIUM CLOUD
WIIT AG
Joachim-Erwin-Platz 3
40212 Düsseldorf
Deutschland

Geltungsbereich: Bereitstellung, Betrieb und Überwachung von Colocation, Web-, Cloud- und Hostingdienstleistungen

SoA V10, 2024-03-06

Durch ein Audit wurde der Nachweis erbracht, dass die Forderungen der ISO/IEC 27001:2022 erfüllt sind.

Gültigkeit: Dieses Zertifikat ist gültig vom 10.06.2024 bis 09.06.2027.
Erstzertifizierung 2024

18.06.2024

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

IAF

DAkkS
Deutsche Akkreditierungsstelle
D-ZM-16031-01-00

TÜVRheinland®
Genau. Richtig.