TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN ZUM SCHUTZ PERSONENBEZOGENER DATEN

Computacenter Group
Managementsystem für Informationssicherheit

Group Information Systems

Dokumentenversion 3.4

- Unbeschränkt -

DOKUMENTENINFORMATIONEN

Angaben zu diesem Dokument	
Thema	Group Data Privacy TOMs
Fassung vom	22.12.2023
Version	3.4
Revisionszyklus	1 Jahr
Klassifikation	Unbeschränkt
Dokumenteigentümer	Group Chief Information Security Officer

INHALTSVERZEICHNIS

EINFÜHRUNG

Dieses Dokument beschreibt die Technischen und Organisatorischen Sicherheitsmaßnahmen, die von Computacenter zum Schutz von Informationen implementiert wurden, und es ist auf alle von Computacenter verwalteten Systeme sowie auf seine Mitarbeiter, Partner und Dritte anwendbar. Siehe Anhang 1 und 2 für weitere Informationen.

Computacenter erfüllt die in der Datenschutz-Grundverordnung (DSGVO) festgelegte Verpflichtung, die Verarbeitung personenbezogener Daten durch geeignete technische und organisatorische Maßnahmen zu sichern und, soweit möglich, personenbezogene Daten zu anonymisieren oder zu pseudonymisieren. Alle getroffenen Maßnahmen berücksichtigen das mit der jeweiligen Datenverarbeitung verbundene Risiko. Insbesondere die Wirksamkeit der Maßnahme berücksichtigt die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität.

DATENSCHUTZ-MANAGEMENT

1 Grundsätze des Datenschutzes

Im Folgenden werden die hochrangigen Prinzipien dargelegt, die den Praktiken von Computacenter für das Sammeln, Verwenden, Offenlegen, Speichern, Sichern, Zugreifen, Übertragen oder die sonstige Verarbeitung personenbezogener Daten zugrunde liegen.

- **Rechtmäßigkeit, Fairness und Transparenz**
  - Computacenter verarbeitet personenbezogene Daten rechtmäßig, nach Treu und Glauben und in transparenter Weise in Bezug auf die betroffene Person, nur für die rechtmäßigen Geschäftszwecke und nur dann, wenn die Verarbeitung erforderlich ist, um unseren gesetzlichen Verpflichtungen nachzukommen.
- **Zweckbindung**
  - Computacenter erhebt personenbezogene Daten nur für einen bestimmten, expliziten und legitimen Zweck.
  - Jede nachfolgende Verarbeitung muss mit diesem/diesen Zweck(en) vereinbar sein, es sei denn, Computacenter hat die Zustimmung der Person eingeholt oder die Verarbeitung ist anderweitig gesetzlich zulässig.
- **Daten-Minimierung**
  - Computacenter stellt sicher, dass die verarbeiteten personenbezogenen Daten angemessen, sachdienlich und auf das für den/die Verarbeitungszweck(e) notwendige Maß beschränkt sind.
- **Begrenzung der Speicherung**
  - Computacenter bewahrt personenbezogene Daten in einer Form auf, die eine persönliche Identifizierung ermöglicht, und zwar nicht länger als notwendig, um den/die Zweck(e) oder andere(n) zulässige(n) Zweck(e), für den/die die personenbezogenen Daten erhoben wurden, zu erfüllen.
- **Richtigkeit**
  - Computacenter unternimmt angemessene Schritte, um ungenaue oder unvollständige Daten zu aktualisieren oder zu entfernen. Einzelpersonen haben das Recht, von Computacenter die unverzügliche Löschung oder Berichtigung der sie betreffenden fehlerhaften Daten zu verlangen.
- **Integrität und Vertraulichkeit**
  - Computacenter speichert personenbezogene Daten sicher und geschützt vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung durch geeignete technische oder organisatorische Maßnahmen.
- **Rechenschaftspflicht**
  - Computacenter legt geeignete Richtlinien, Prozesse, Kontrollen und andere Maßnahmen fest, die erforderlich sind, damit nachgewiesen werden kann, dass seine Verarbeitung personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen erfolgt.

1.1 Informationssicherheitsfunktion

- Computacenter verfügt über eine etablierte Group Information Systems-Funktion, die vom Group Chief Information Security Officer (Group CISO) geleitet wird. Der Group CISO ist dafür verantwortlich, die Implementierung von Informationssicherheitselementen wie Rahmenwerk, Richtlinien, Prozesse und Konformitätsmaßnahmen sicherzustellen;

- Der Group CISO wird von einem Team unterstützt, das auf Geschäftseinheiten und geografische Gebiete ausgerichtet ist;
- Der Group CISO stimmt sich mit dem Datenschutzbeauftragten der Gruppe in Bezug auf die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten ab;
- Computacenter hat ein Informationssicherheits-Managementsystem (ISMS) eingerichtet, das auf den internationalen Best Practices von ISO/IEC 27001:2013 und verwandten Sicherheitsstandards basiert;
- Das ISMS wurde und wird weiterhin von Auditoren bewertet und erhält regelmäßig eine Zertifizierung gemäß ISO/IEC 270001:2013; und
- Computacenter verfügt über eine umfassende Reihe von Informationssicherheitsrichtlinien, die von der Unternehmensleitung genehmigt und allen Mitarbeitern zugänglich gemacht werden.

Die Hauptziele von Computacenter in Bezug auf die Informationssicherheit sind:

- Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der gespeicherten oder verarbeiteten internen Daten und Kundendaten, es sei denn, das Unternehmen ist zur Offenlegung berechtigt oder anderweitig gesetzlich verpflichtet.
- Die Verantwortung für die Verhinderung, Erkennung und Meldung von Datenverlusten und anderen Unternehmens- oder Kunden-Assets zu übernehmen.
- Sicherstellen, dass Aktivitäten im Zusammenhang mit der Informationssicherheit auf vertrauenswürdige, verantwortungsvolle und effektive Weise durchgeführt werden und durch eingebettete Prozesse nachhaltig sind.
- Unseren Kunden weiterhin sichere Services, Lösungen und Produkte in einer sicheren Umgebung zur Verfügung zu stellen und die Sicherheit in wesentliche Geschäftsprozesse zu integrieren.
- Durchführung regelmäßiger Risikobewertungen im Bereich der Informationssicherheit, um sicherzustellen, dass Sicherheitsrisiken auf konsistente und wirksame Weise behandelt werden, die Wahrscheinlichkeit des Auftretens von Vorfällen im Bereich der Informationssicherheit zu verringern und deren potenzielle Auswirkungen auf das Geschäft und die Kunden zu begrenzen.
- Die fachlichen Kompetenzen unserer Mitarbeiter:innen und Zulieferer in Bezug auf die Informationssicherheit weiter zu verbessern.
- Sicherstellen, dass unser Managementsystem für Informationssicherheit (ISMS) uns dabei unterstützt, unsere Effizienz und Effektivität zu verbessern und eine Kultur der kontinuierlichen Verbesserung der Informationssicherheit zu fördern, um das Vertrauen der Kunden in Computacenter zu stärken und so dazu beizutragen, Aufträge zu gewinnen und zu erhalten.

2. Privacy by Design und by Default

2.1. Anonymisierung & Pseudonymisierung (Artikel 32 (1a), Artikel 25 (1) DSGVO)

- Anonymisierung, Pseudonymisierung und Minimierung personenbezogener Daten sind für neue Informationsverarbeitungsaktivitäten in Übereinstimmung mit den Grundsätzen eines "Privacy by Design"/"Security by Design"-Prozesses in Betracht zu ziehen, der darauf abzielt, bewährte Verfahren für Sicherheit und Datenschutz in die Systementwürfe zu integrieren, wo dies möglich ist; und

- Auf der Grundlage der Ergebnisse der Risikobewertung werden Mindestmaßnahmen für den Einsatz von Kryptographie, wie z.B. Verschlüsselung, in Übereinstimmung mit Computacenter Richtlinien und Standards, in Betracht gezogen.

2.2. Anpassung an globale Standards

- Computacenter hat eine Reihe von Sicherheitszertifizierungen erreicht; Informationssicherheitsrichtlinien und -standards wurden entwickelt, um die Anforderungen von ISO/IEC 27001:2013 zu erfüllen; und
- Die kundenorientierten Systeme von Computacenter gehören ebenso zu diesen Zertifizierungen wie die internen Technologien, die von den Benutzern verwendet werden und die von seinem Group Information Systems Team bereitgestellt werden.

2.3. Gewährleistung von Sicherheit und Datenschutz

- Neue Datenverarbeitungsaktivitäten werden intern bewertet, und Datenminimierung und "Privacy by Design“ und „Privacy by Design" werden innerhalb des Design- und Entwicklungsprozesses für neue Anwendungen oder Systeme berücksichtigt; und
- Besteht für die betroffene Person, die von den Datenverarbeitungstätigkeiten betroffen ist, ein hohes Risiko, so wird eine Datenschutz-Folgenabschätzung durchgeführt, und die Fragen werden zur Zufriedenheit des/der zuständigen Datenschutzbeauftragten oder, wenn im Zusammenhang mit einer solchen Verarbeitung weiterhin ein hohes Risiko für die betroffenen Personen besteht, in Absprache mit der zuständigen Aufsichtsbehörde behandelt.

2.4. Rechte der betroffenen Personen

- Die Rechte der betroffenen Personen werden durch das Verfahren der Datenschutz-Folgenabschätzung von Computacenter gewährleistet, das sicherstellt, dass die Verarbeitung personenbezogener Daten durch Computacenter diese Rechte in dem Maße erfüllt, wie sie anwendbar sind.

3. Verfahren zur regelmäßigen Prüfung, Beurteilung und Bewertung der Wirksamkeit (Artikel 32 (1d), Artikel 25 (1) DSGVO)

3.1. Interne Audits

- Als Teil der ISO/IEC 27001:2013-Zertifizierung gibt es vollständige interne und externe Auditprogramme, um sicherzustellen, dass Verstöße erkannt und bis zur Lösung gehandhabt werden;
- Externe Audits werden mindestens jährlich und interne Audits kontinuierlich durchgeführt, um die Einhaltung von ISO/IEC 27001:2013 sicherzustellen; und
- Die Ergebnisse werden in Form eines Auditberichts festgehalten.

3.2. Risikomanagementprogramm von Drittanbietern

- Drittanbieter, die personenbezogene Daten im Auftrag von Unternehmen der Computacenter Gruppe verarbeiten, sind verpflichtet, bestimmten vertraglichen Bestimmungen zuzustimmen, die Computacenters Verpflichtungen als (Daten)Verantwortlicher oder (Daten)Verarbeiter dieser personenbezogenen Daten wiederspiegeln;
- Die Leistungsfähigkeit der Informationssicherheit von Drittanbietern wird von Computacenters Group Information Systems-Funktion auf der Grundlage der von diesem Anbieter erbrachten Dienstleistungen und der damit verbundenen Risiken im Zusammenhang mit einem Verstoß bewertet; und
- Eine Datenverarbeitung durch Dritte ist ohne vertragliche Vereinbarungen zur Einhaltung der Vorschriften bei der Datenverarbeitung nicht zulässig.

3.3. Sichere Konfiguration

- Computacenter führt regelmäßige Überprüfungen durch, um sicherzustellen, dass die sichere Konfiguration der Geräte den Anforderungen der Informationssicherheitsrichtlinien entspricht;
- Schwachstellen-Scans und Penetrationstests werden eingesetzt, um die Nichteinhaltung von Sicherheitsrichtlinien zu erkennen und innerhalb vereinbarter Zeiträume zu beheben;
- Ein geplantes Betriebssystem-Patching-Programm behebt Systemfehler gemäß den vom Hersteller veröffentlichten Zeitplänen;
- Gegebenenfalls ist die Möglichkeit der Benutzer, die Konfiguration von Systemen zu ändern, deaktiviert;
- Standardisierte Server- und Betriebssystem-Builds werden in Übereinstimmung mit Industriestandards konfiguriert, um gegen Angriffe resistent zu sein; und
- Die Konfiguration von Systemen, die personenbezogene Daten verarbeiten, werden vor der Freigabe in der Produktionsumgebung validiert.

Anhang 1 - Technische Sicherheitsmaßnahmen

Logische Zugriffskontrolle

- Alle Benutzer greifen auf Computacenter-Systeme mit einer eindeutigen Kennung zu;
- Generische Konten sind verboten, es sei denn, es liegt eine geschäftsbezogene Begründung vor und eine Ausnahme von der beantragten Richtlinie wurde genehmigt;
- Benutzer müssen ein sicheres Kennwort oder ein anderes Mittel zur Authentifizierung wählen, das der die im Standard für die Verwaltung von Authentifizierungsinformationen definierten Anforderungen an Authentifizierungsinformationen entspricht;
- Regeln für den Ablauf und die Wiederverwendung von Passwörtern sind gemäß den in dem Standard für die Verwaltung von Authentifizierungsinformationen festgelegten Anforderungen vorkonfiguriert;
- Benutzerkonten für Anwendungen sind mit einem automatischen Abmeldeprozess konfiguriert, und Betriebssysteme sind so konfiguriert, dass sie Konten nach einer bestimmten Zeit der Inaktivität sperren;
- Für den Fernzugriff auf Systeme ist eine Zwei-Faktor-Authentifizierung implementiert;
- Rollenbasierte Zugriffskontrolle wird in allen Kernsystemen eingesetzt;
- Computacenter arbeitet mit dem Modell des Zugriffs mit den geringsten Privilegien für jeden Mitarbeiter; vor Umsetzung muss zusätzlicher Zugriff vom Vorgesetzten des Mitarbeiters und den System-/Service-Eigentümern genehmigt werden;
- Computacenter verfügt über ein umfassendes Verfahren zur Deaktivierung von Benutzern und deren Zugang, wenn Mitarbeiter das Unternehmen oder eine Funktion verlassen; und
- Jeder Zugriff oder versuchte Zugriff auf Systeme wird protokolliert und überwacht.

Implementierte Anforderung an die Datentrennung zum Schutz der Vertraulichkeit

- Die Umgebungen für die Shared-Service-Plattformen, die Computacenter seinen Kunden zur Verfügung stellt, sind getrennt und in Übereinstimmung mit den Grundsätzen bewährter Sicherheitspraktiken implementiert;
- Die Datenverarbeitung in jeder Umgebung wird für jeden Kunden separat durchgeführt (logische oder physische Trennung); und
- Die Zugriffsrechte werden durch geeignete Gruppierungen und die damit verbundene Rechteverwaltung kontrolliert, um eine logische Datentrennung zwischen den Kunden zu gewährleisten;

Datentransfer-Kontrollen zur Gewährleistung der Integrität der Systeme (Artikel 32 (1b) DSGVO)

Kontrolle von Wechseldatenträgern

- Die Übertragung oder Speicherung personenbezogener Daten auf oder von Mobiltelefonen, DVD/CD- oder USB-Speichersticks erfolgt in Übereinstimmung mit der Richtlinie zum angemessenen Umgang mit Informationen sowie der Matrix zur Klassifizierung und Handhabung von Informationen von Computacenter; und

- Wechselmedien zur Speicherung persönlicher Daten dürfen nicht für geschäftliche Zwecke verwendet werden, es sei denn, es werden fallspezifische Ausnahmen beantragt und eine Genehmigung erteilt.

Übertragung von webbasierten Anwendungsdaten

- Der elektronische Datenaustausch innerhalb des Unternehmens ((bzw., wo vereinbart, mit unseren Kunden und Lieferanten) erfolgt über verschlüsselte Verbindungen (einschließlich SSL/IPSec VPNs, TLS) und dedizierte Leitungen, wodurch die Integrität und Vertraulichkeit der Informationen während der Übertragung gewährleistet wird.

Netzwerk-Sicherheit

- Innerhalb von Computacenter und zwischen Computacenter und seinen Kunden und Lieferanten sind Vorkehrungen vorhanden, um den Datentransfer über verschlüsselte Verbindungen (TLS, SSL, IPSec) und dedizierte Schaltungen durchzuführen;
- Gastnetzwerke sind von den Computacenter-Kernnetzwerken abgetrennt;
- Schwachstellenscans werden durch interne Netzwerkscans im gesamten Netz durchgeführt;
- Regelmäßige Überprüfungen der Systeme durch Dritte werden durch Penetrationstests durchgeführt; und
- Die Verwaltung von Netzwerkkomponenten und -geräten ist auf diejenigen beschränkt, die über die entsprechenden Berechtigungen für die Verwaltung dieser Systeme verfügen.

Mobiles Arbeiten

- Mitarbeitern und Auftragnehmern der Computacenter werden Firmengeräte und relevante Sicherheitsmethoden für Fernverbindungen zur Verfügung gestellt;
- Ein Zwei-Faktor-Authentifizierungsverfahren ist erforderlich, um den Firmenlaptop mit dem Netzwerk zu verbinden; und
- Die Benutzer sind verpflichtet, die Richtlinie zum angemessenen Umgang mit Informationen von Computacenter einzuhalten.

Implementierte Kontrollen zum Schutz der Integrität der Systeme

Monitoring

- Computacenter betreibt eine SIEM-Lösung (Security Information and Event Monitoring), die 24x7 unterstützt wird, um Sicherheitsereignisse zu erkennen;
- Protokolle und Ereignisse werden täglich über die SIEM-Plattform überprüft, wobei ein spezielles Team für die Protokollüberprüfung/-analyse und die Behandlung von Alarmen/Vorfällen bzw. Eskalationen, falls erforderlich, zugewiesen und geschult wird;
- Ereignisse auf System- und Netzwerkebene werden überwacht, protokolliert und analysiert, und Vorfälle werden mit entsprechenden Prioritäten gemeldet. Solche Vorfälle werden durch den Prozess des Managements von Sicherheitsvorfällen gehandhabt; und
- Die Protokollierung der Benutzeraktivitäten erfolgt in Übereinstimmung mit der Richtlinie für Protokollierung und Überwachung sowie dem Standard für Sicherheitsprotokollierung und Ereignisüberwachung.

Klassifizierung und Handhabung von Dokumenten

- Alle Daten innerhalb der Computacenter-Gruppe werden durch Bezugnahme auf und in Übereinstimmung mit der Richtlinie zum angemessenen Umgang mit Informationen sowie der Matrix zur Klassifizierung und Handhabung von Informationen von Computacenter klassifiziert und verwendet; und
- Personenbezogene Daten werden in Übereinstimmung mit der Richtlinie zum angemessenen Umgang mit Informationen sowie der Matrix zur Klassifizierung und Handhabung von Informationen klassifiziert basierend auf der Risikogrundlage für betroffene Personen, die mit einer Sicherheitsverletzung verbunden sind, die zu einem Verlust solcher personenbezogenen Daten führt.

Maßnahmen zum Schutz der Verfügbarkeit und Belastbarkeit der Systeme (Artikel 32 (1b) DSGVO)

Datensicherung

- Computacenter unterhält Backups der Kernsysteme unter Verwendung virtueller Bandtechnologie, die über die Rechenzentren hinweg repliziert wird.

Malware-Schutz

- Zum Schutz der Komponenten der Infrastruktur und der Endgeräte sind Antiviren-Systeme implementiert;
- Das Echtzeit-Virenscannen ist aktiviert, und es werden regelmäßig geplante Scans auf den Endgeräten durchgeführt;
- Externe E-Mails werden gefiltert, um eine zusätzliche Hygienestufe einschließlich Anti-Spam, Anti-Phishing und Anti-Virus-Scanning zu erreichen.

Maßnahmen zur Unterstützung der Wiederherstellung nach Notfällen

- Der IT-Risikomanagement- und Business-Continuity-Prozess von Computacenter stellt sicher, dass Programme, Konfigurationen und Daten in Übereinstimmung mit definierten Prozessen und Vorschriften verfügbar gehalten werden;
- Im Falle eines Versagens (Katastrophe, Unfall) sind die neuesten Maßnahmen in Kraft, um die Wiederherstellung und weitere Nutzung zu gewährleisten;
- Computacenter verfügt über lokalisierte Krisenmanagement-Fähigkeiten, die in den Prozeduren für den Prozess des Managements schwerer Zwischenfälle und des Business Continuity Managements spezifiziert sind,
- Eine detaillierte Wiederherstellungsdokumentation sind für alle Kernsysteme verfügbar, um im Falle eines Zwischenfalls eine schnelle Wiederherstellung des Normalbetriebs zu gewährleisten;
- Regelmäßige individuelle Wiederherstellungstests werden durchgeführt, wobei die Wiederherstellungspläne bei Bedarf aktualisiert werden; und
- Die Wiederherstellungsverfahren unterliegen der internen Revisionskontrolle. Die Rechenzentren der Computacenter Group sind mit der neuesten Ausfallsicherheitstechnologie ausgestattet.

Anhang 2 - Organisatorische Sicherheitsmaßnahmen

Beschränkungen bei der Speicherung und Aufbewahrung

- Personenbezogene Daten werden in einer Form, die die Identifizierbarkeit der betroffenen Personen ermöglicht, nicht länger aufbewahrt, als es für den/die Zweck(e), für die die personenbezogenen Daten verarbeitet werden, erforderlich ist;
- Die Festlegung der Anforderungen an die Datenspeicherung in Bezug auf personenbezogene Daten, die für die Erbringung von Dienstleistungen verarbeitet werden, liegt in der Verantwortung des Kunden; und
- Personenbezogene Daten werden vernichtet oder nach Ablauf der entsprechenden Datenaufbewahrungsfrist an einen Kunden zurückgegeben.

Informationssicherheit und Datenschutz, Sensibilisierung und Schulung

- Schulungen zur Informationssicherheit und zum Datenschutz stehen den Computacenter-Mitarbeitern über das Lernmanagementsystem des Unternehmens zur Verfügung; und
- Die Mitarbeiter von Computacenter werden beim Eintritt in Computacenter und danach in regelmäßigen Abständen zu Pflichtschulungen angemeldet.

Mitarbeiter-Screening

- Überprüfungen vor der Einstellung werden als Teil der Prozesse der Personalbeschäftigung durchgeführt; und
- Zusätzliche Überprüfungen können für bestimmte Positionen oder die Anforderungen einzelner Kunden erforderlich sein, wenn die örtlichen Gesetze dies zulassen.

Prozesse für Eintritte, Wechsel und Abgänge von Mitarbeitern

- Der sogenannte Joiner/Mover/Leaver-Prozess steuert die Zugriffsrechte, die einem Benutzer während seiner Beschäftigung bei der Organisation zugewiesen werden;
- Wenn ein Mitarbeiter Computacenter verlässt, wird das Benutzerkonto sofort durch einen automatisierten Prozess deaktiviert.

Management von Informationssicherheitsvorfällen und Datenschutzverletzungen

- Innerhalb von Computacenter ist Informationssicherheit-Managementprozess eingerichtet, um Vorfälle zu identifizieren, zu untersuchen und bis zur Lösung zu verwalten;
- Sicherheitsvorfälle und potenzielle Datenschutzverletzungen werden durch den Prozess des Managements von Sicherheitsvorfällen behandelt; und
- Datenschutzverletzungen werden dem zuständigen Datenschutzbeauftragten und den betroffenen Kunden über den Prozess des Managements von Sicherheitsvorfällen umgehend und ohne unangemessene Verzögerung mitgeteilt.

Maßnahmen des physischen Zutritts zum Schutz der Vertraulichkeit

- Computacenter hat für jedes seiner Gebäude definierte physische Sicherheitszonen, um die physischen Sicherheitsmaßnahmen zu kontrollieren;
- Jede Sicherheitszone wird durch elektronische Zutrittssysteme, und bestimmte Bereiche werden durch Wachpersonal überwacht, und es finden Personenkontrollen beim Verlassen der Bereiche statt.
- Besucher der Räumlichkeiten erhalten einen vorläufigen Ausweis und werden immer von einem Mitarbeiter von Computacenter begleitet;
- Rechenzentren verfügen über einen definierten und geschützten physischen Perimeter, physische Kontrollen einschließlich Zugangskontrollmechanismen, kontrollierte Liefer- und Ladebereiche, Überwachung und Sicherheitspersonal;
- Zugang zu Rechenzentren, in denen Kundendaten verarbeitet werden, wird durch Sicherheitsregistrierungsprozesse kontrolliert, für die ein Lichtbildausweis erforderlich ist; und
- Rechenzentren, die Kundendaten verarbeiten, werden vor Stromausfällen und anderen Unterbrechungen geschützt, und es sind Branderkennungs- und -bekämpfungssysteme implementiert.

Schutz streng vertraulicher Daten

- Computacenter arbeitet bei der Handhabung streng vertraulicher Informationen nach dem Need-to-Know-Prinzip;
- Die Richtlinie zum angemessenen Umgang mit Informationen sowie die Matrix zur Klassifizierung und Handhabung von Informationen, die innerhalb von Computacenter veröffentlicht sind, enthalten spezifische Maßnahmen zum Umgang mit streng vertraulichen Informationen, einschließlich Anforderungen an die Dokumentenverschlüsselung;
- Die Richtlinie zum angemessenen Umgang mit Informationen legt fest, welche persönlichen Daten als streng vertraulich eingestuft werden
- Der Austausch streng vertraulicher Informationen mit Dritten muss in Übereinstimmung mit der Computacenter Matrix zur Klassifizierung und Handhabung von Informationen durchgeführt werden; und
- Der Risikomanagementprozess wird in Zusammenarbeit mit den Dateneigentümern und Datenverwaltern die Risiken im Zusammenhang mit Daten, die besondere Sorgfalt erfordern, bewerten und verwalten