DATAGROUP

DATAGROUP TOM

Verfahrensbeschreibung der technisch-organisatorischen Maßnahmen im Sinne von Art.32 Abs.1 DSGVO

Änderungshistorie

In der nachfolgenden Tabelle werden alle Änderungen an diesem Dokument mit Versionsnummer, Datum der Änderung sowie Gültigkeit, Bearbeiter und Beschreibung der Änderung dokumentiert. Überprüfungen ohne Änderungen werden ebenfalls dokumentiert. Die Version ist in diesem Fall gleich zu behalten.

Achtung: Nach Änderungen muss in der Fußzeile des Dokuments die Versionsnummer angepasst werden.

Versions-Nr.	Datum der Änderung / Überprüfung	Bearbeiter	Beschreibung der Änderung
1.0	02.03.2018	Datenschutz süd (CQ)	Erstellung Konzept nach DSGVO
2.0	27.04.2020	M. Clar	Umstellung auf neues Layout Überarbeitung von Formulierungen Aufnahme neuer Einheiten Konsolidierung der Rechenzentrumsmaßnahmen Freigabe durch CSB am 28.04.2020
2.1	13.07.2020	Jörg Angerer	Namensänderung DSB
2.2	25.11.2020	Jörg Angerer	Vertraulichkeitsstufe auf intern geändert. Kapitel 3.2.3: Zutritte protokolliert, Notausgänge alarmgesichert
2.3	13.01.2021	Christian Dugall	Erwähnung der ISO 27018 in Kapitel 1
2.4	28.01.2021	Jörg Angerer	DATAGROUP Consulting nach Verschmelzung mit DATAGROUP IT Solutions entfernt.
2.5	10.12.2021	Jörg Angerer	Aufnahme DATAGROUP BIT Düsseldorf
2.6	23.05.2022	Jörg Angerer	Ergänzung Kapitel 8.3
2.7	19.10.2022	Jörg Angerer	Aktualisierung Vorstände

2.8	09.03.2023	Jörg Angerer	Aufnahme weiterer Gesellschaften, Neues Kapitel 9 Mobiles Arbeiten , Rechenzentrum-Standorte aktualisiert, technische Neuerungen in Kapitel 6 ergänzt
2.9	06.05.2024	Manfred Clar, Jörg Angerer	Korrektur Vorstand und Aufnahme weiterer Gesellschaften Kap. 2, Auflistung RZ-Standorte entfernt, Aktualisierung Kap. 3.3.2

Inhaltsverzeichnis

Information zum Dokument

Stellung des Dokuments

Das vorliegende Dokument enthält eine Übersicht über die bei DATAGROUP gemäß Art.32 Abs.1 DSGVO umgesetzten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.
Das Dokument wird beim Abschluss von Verträgen zur Auftragsverarbeitung als Anlage eingefügt.

Gültigkeit

Dieses Dokument wird mindestens jährlich auf seine Aktualität überprüft. Überprüfungen und Aktualisierungen werden in der Dokumentenhistorie dokumentiert. Kopien und Ausdrucke unterliegen dabei nicht der Aktualisierung.
Die aktuell gültige Version ist im DATAGROUP KnowledgeCenter veröffentlicht.

Hinweis

DATAGROUP setzt sich für die Gleichbehandlung aller Geschlechter ein. Die mögliche Verwendung des generischen Maskulinums in diesem Dokument dient lediglich der Vereinfachung, in allen Fällen sind stets männliche, weibliche und diverse Personen gemeint.

Verantwortlichkeiten

Rolle, Funktion	Name	Kontaktdaten
Verantwortlich für das vorliegende Dokument		
CISO	Mark Schäfer	Mark.Schaefer@datagroup.de

1 Einleitung

Alle Stellen, die personenbezogene Daten verarbeiten, sind gemäß Art.32 Abs.1 EU Datenschutzgrundverordnung (DSGVO) verpflichtet, 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 geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau für die Rechte und Freiheiten natürlicher Personen zu gewährleisten.

Dieses Dokument enthält eine Übersicht über die bei DATAGROUP gemäß Art.32 Abs.1 DSGVO hierzu umgesetzten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.

DATAGROUP überprüft die getroffenen technischen und organisatorischen Maßnahmen regelmäßig daraufhin, ob sie dem Stand der Technik und den organisatorischen Möglichkeiten entsprechen. Insoweit ist es DATAGROUP gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei ist gewährleistet, dass das Sicherheitsniveau der in diesem Dokument festgelegten Maßnahmen nicht unterschritten wird.

Zur Sicherstellung der Informationssicherheit - Vertraulichkeit, Verfügbarkeit und Integrität sämtlicher Informationen - für DATAGROUP und deren Kunden wurde das DATAGROUP ISMS (Information Security Management System) gemäß ISO/IEC 27001 für alle Unternehmen im Konzernverbund der DATAGROUP SE implementiert.

Das DATAGROUP ISMS ist für DATAGROUP SE und ausgewählte DATAGROUP Gesellschaften und Services gemäß ISO/IEC 27001 mit ISO 27018 Erweiterung zertifiziert und wird regelmäßigen internen und externen Überprüfungen unterzogen.

Des Weiteren sind Hosting- und Outsourcing-Projekte der DATAGROUP Operations GmbH gemäß ISO 27001 auf der Basis von IT-Grundschutz sowie BSI C5 zertifiziert.

2 Organisatorische und rechtliche Struktur

DATAGROUP ist eines der führenden IT-Dienstleistungsunternehmen in Deutschland. Unter dem Dach der DATAGROUP SE sind die operativ tätigen Tochtergesellschaften angeordnet. Das vorliegende Dokument hat Gültigkeit für folgende Gesellschaften:

DATAGROUP SE (Holding), Pliezhausen
Vorstand: Andreas Baresel (CEO), Sabine Laukemann

ALMATO AG

Almato AI

Almato Iberia

DATAGROUP Polska Sp. z o.o.

DATAGROUP BIT Düsseldorf GmbH

DATAGROUP BIT Hamburg GmbH

DATAGROUP Banking Operations Center s.r.o.

DATAGROUP Bremen GmbH

DATAGROUP Business Solutions GmbH mit den Geschäftsbereichen

- DATAGROUP Berlin
- DATAGROUP Business Solutions neu
- DATAGROUP Defense IT Services
- DATAGROUP München

DATAGROUP Consulting Services GmbH

DATAGROUP Cyber Security GmbH

DATAGROUP Enterprise Services GmbH

DATAGROUP Enterprise Services Kft

DATAGROUP Frankfurt GmbH

DATAGROUP Hamburg GmbH

DATAGROUP Inshore Services GmbH

DATAGROUP IT Solutions GmbH

DATAGROUP Köln GmbH

DATAGROUP Ludwigsburg GmbH

DATAGROUP Offenburg GmbH

DATAGROUP Operate IT GmbH

DATAGROUP Operations GmbH

DATAGROUP Service Desk GmbH

DATAGROUP Stuttgart GmbH

DATAGROUP Ulm GmbH

Hövermann IT-Gruppe GmbH

Mercoline GmbH

systemzwo GmbH mit kraftwerk 3 IT GmbH

URANO Informationssysteme GmbH

DATAGROUP betreibt ihre Systeme in mehreren Rechenzentren in Deutschland. Die in diesem Dokument beschriebenen Maßnahmen gelten für alle Rechenzentren.

Die nachfolgend aufgeführten Maßnahmen beziehen sich – soweit nicht anders angegeben – auf alle Standorte der DATAGROUP Gesellschaften im Scope dieses Dokumentes. Diese Standorte befinden sich größtenteils in Deutschland sowie vereinzelt im EU-Ausland.

3 Vertraulichkeit

3.1 Erläuterung

Nach Art.5 Abs.1lit. f), Art.32 Abs.1 lit.b) DSGVO ist die Vertraulichkeit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen zu gewährleisten. Die Daten sind vor unbefugter Kenntnisnahme und vor unbefugter oder unrechtmäßiger Verarbeitung zu schützen. Es sind hierfür Maßnahmen gegen den unbefugten Zutritt, Zugang und Zugriff auf das System sowie zur Trennung der Datenverarbeitungen zu etablieren. Ferner ist durch geeignete Maßnahmen die Weitergabe von Daten zu kontrollieren.

3.2 Zutrittskontrolle

3.2.1 Erläuterungen

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

3.2.2 Maßnahmen für alle DATAGROUP Standorte

Alle Gebäudeeingänge der DATAGROUP-Standorte sind mit elektronischen Zutrittssystemen gesichert. Räume mit erhöhtem Schutzbedarf sind mit zusätzlichen Sicherheitsschlössern ausgestattet. Es besteht eine Schlüsselregelung, die jeweils lokal dokumentiert ist.

Sensible Bereiche der Gebäude sind videoüberwacht und / oder mit einer Einbruchmeldeanlage gesichert.

Personen, die nicht der DATAGROUP angehören, werden persönlich am Eingang abgeholt und innerhalb der Räumlichkeiten der DATAGROUP begleitet.

3.2.3 Ergänzende Maßnahmen bei Standorten mit Rechenzentrum

Für die DATAGROUP Rechenzentren sind folgende zusätzliche Maßnahmen getroffen:

- Die Rechenzentren sind ISO 27001 bzw. DIN EN 50600 (RZ Ibbenbüren) zertifiziert.
- Alle Außentüren werden stets verschlossen gehalten und sind mit einem elektronischen Zutrittskontrollsystem gesichert.
- Die zutrittsberechtigten Personen und ihre Befugnisse sind namentlich dokumentiert.
- Die Berechtigungen unterliegen einem regelmäßigen dokumentierten Review.
- Berechtigungsänderungen müssen schriftlich beantragt werden. Der Ablauf ist in einer Verfahrensbeschreibung dokumentiert.
- Es sind mehrere Sicherheitszonen eingerichtet.
- Alle äußeren Zugänge werden videoüberwacht. Die Videoaufnahmen werden für definierte Zeiträume aufbewahrt.
- Alle Zutritte innerhalb des Rechenzentrums werden protokolliert.
- Die Zutrittsprotokolle unterliegen einem regelmäßigen dokumentierten Review.
- Besucher und sonstige firmenfremde Personen müssen sich anmelden und ausweisen.
- Besucher und sonstige firmenfremde Personen werden persönlich am Eingang abgeholt und innerhalb des Rechenzentrums begleitet.
- Mitarbeiter und Besucher müssen immer sichtbar einen Ausweis tragen.
- Das Rechenzentrum ist mit einer Einbruchmeldeanlage (mit optionaler Rack-Überwachung) gesichert.

- Notausgänge sind alarmgesichert.
- Es werden regelmäßige Kontrollrundgänge des Sicherheitsdienstes durchgeführt.
- Die Türen weisen eine ausreichende Widerstandsklasse (mind. F90) und Sicherheitsschlösser auf.
- Fenster sowie Licht- und Lüftungsschächte sind vergittert.
- Die Fenster haben eine einbruchhemmende Verglasung.

3.3 Zugangskontrolle

3.3.1 Erläuterung

Um die Vertraulichkeit der Datenverarbeitung zu gewährleisten, ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

3.3.2 Maßnahmen

Der Zugang zu den IT-Systemen von DATAGROUP erfolgt über individuell vergebene Zugangskennungen.

Zugangskennungen bestehen aus Benutzername und Passwort. Sie werden nach einem definierten Prozess auf Antrag vergeben. Für die Vergabe besteht ein Berechtigungskonzept.

Vergebene Benutzerkonten und Zugriffsberechtigungen werden im Rahmen der Benutzerkontenverwaltung regelmäßig überprüft und ggf. angepasst oder gelöscht.

Es besteht eine Regelung für die Erstellung und Verwendung von Passwörtern (DATAGROUP Richtlinie Passwortmanagement).

- Mindestlänge 12 Zeichen
- mindestens eine Ziffer, ein Sonderzeichen, ein Großbuchstabe und ein Kleinbuchstabe
- maximale Gültigkeit von 180 Tagen
- Die letzten zehn Passwörter können nicht erneut verwendet werden
- Triviale Passwörter sind nicht gestattet und werden durch das System im Rahmen des technisch Möglichen unterbunden (z.B. durch Verwendung eines Wörterbuchs)
- Vergebene Passwörter sind geheim zu halten und dürfen in Dateien, Anwendungen oder Webbrowsern nicht gespeichert werden. Es wird ein zentrales Passwort-Safe-Tool zur Verfügung gestellt

Die Anzahl erlaubter Anmeldeversuche ist begrenzt.

Nach einem definierten Zeitraum der Inaktivität eines Benutzers wird die passwortgeschützte Bildschirmsperre automatisch aktiviert. Bei Verlassen des Arbeitsplatzes ist die passwortgeschützte Bildschirmsperre durch den Benutzer manuell zu aktivieren.

Es besteht eine Clean Desk-Policy. Die Beschäftigten sind verpflichtet, Ausdrucke oder Kopien unverzüglich aus Druckern oder Kopiergeräten zu entnehmen. Unterlagen mit personenbezogenen Daten oder vertraulichen Informationen dürfen auf Schreibtischen nicht offen zugänglich hinterlassen werden.

Bildschirme und Drucker sind grundsätzlich so aufgestellt, dass sie gegen Einblicke unbefugter Dritter geschützt sind.

Administrative Passwörter sind grundsätzlich in einem zentralen System „Password Safe“[1] hinterlegt, der Zugriff erfolgt personifiziert und wird protokolliert.

Der administrative Zugang auf die Systeme in den Rechenzentren erfolgt aus einer Management- und Administrationsumgebung heraus. Diese ist in Form einer separaten Umgebung realisiert, die sowohl losgelöst von den Mandantenumgebungen als auch von der DATAGROUP Office-Umgebung ist. Der Zugriff auf die Mandantenumgebungen erfolgt via VPN-Verbindung oder Jumpserver und sieht eine vorgeschaltete Authentisierung mittels separater Benutzer vor.

Der ein- und ausgehende Datenverkehr mit dem Unternehmensnetzwerk wird durch eine Firewall überwacht und eingeschränkt. Die Firewall wird regelmäßig gewartet.

Für die Diagnose und Konfiguration von IT-Systemen sind nur bestimmte IP-Bereiche und Ports freigegeben.

Die Nutzung mobiler Systeme ist reglementiert. Der Zugriff auf das Unternehmensnetzwerk von außen erfolgt grundsätzlich über SSL-verschlüsselte Terminalserver-Sitzungen bzw. unter Verwendung verschlüsselter VPN-Verbindungen inkl. 2-Faktor-Authentifizierung (2FA). Für einen längeren Zeitraum inaktive VPN-Verbindungen werden unterbrochen.

Die von den einzelnen Standorten der DATAGROUP betriebenen Funknetzwerke sind mindestens mit dem Verschlüsselungsalgorithmus Wi-Fi Protected Access 2 (WPA2) gesichert.

3.4 Zugriffskontrolle

3.4.1 Erläuterung

Es ist zu gewährleisten, dass Daten ausschließlich auf Basis von Zugriffsberechtigungen laut Berechtigungskonzept verarbeitet werden und somit personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

[1] Password Safe stellvertretend als Toollösung

3.4.2 Maßnahmen

DATAGROUP realisiert die Benutzerkontenverwaltung über das Active Directory und setzt ein umfassendes Berechtigungskonzept zur Gewährleistung des Minimalprinzips ein.

Eine Vergabe von Zugriffsberechtigungen erfolgt nach dem Need-to-know-Prinzip. Beschäftigte erhalten damit nur Zugriff auf diejenigen Daten, deren Kenntnis im Rahmen der ihnen übertragenen Aufgaben notwendig ist.

Der Zugriff auf Systemsoftware ist ausschließlich Administratoren gestattet.

Die Nutzung privater Datenträger ist für alle Mitarbeiter untersagt.

Die Entsorgung von Datenträgern (Sicherungsmedien und Festplatten) erfolgt grundsätzlich durch qualifizierte Dienstleister im Rahmen einer Auftragsverarbeitung nach Art.28 DSGVO.

3.5 Trennungsgebot

3.5.1 Erläuterung

Im Rahmen des Trennungsgebots ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

3.5.2 Maßnahmen

Die von DATAGROUP betreuten Kundenumgebungen werden in strikt voneinander getrennten Netzwerksegmenten vorgehalten. Sicherungskopien werden in physisch abgetrennten, zugangsgeschützten Bereichen gelagert.

Soweit möglich, werden mandantenfähige Anwendungen eingesetzt.

3.6 Weitergabekontrolle

3.6.1 Erläuterung

Im Rahmen der Weitergabe von personenbezogenen Daten ist zu gewährleisten, dass diese bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern 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.

3.6.2 Maßnahmen

Für die Datenübertragung werden dem Stand der Technik entsprechende Verschlüsselungstechnologien angewendet.

Die Aktivitäten des Administrators auf einem Server werden protokolliert. Die Aufzeichnungen werden für definierte Zeiträume aufbewahrt.

Alle Beschäftigten und zur Leistungserbringung eingesetzte Drittdienstleister sind auf die Vertraulichkeit der Datenverarbeitung und die Einhaltung der Datenschutzvorschriften verpflichtet.

Die Weitergabekontrolle wird durch die Einschränkung der Zugriffsrechte im Rahmen der Benutzerkontenverwaltung mittels Active Directory unterstützt.

Die Nutzung von Internet und E-Mail am Arbeitsplatz ist für die Beschäftigten in der DATAGROUP S2 Benutzerrichtlinie verbindlich geregelt.

Nicht mehr benötigte Datenträger und Papierdokumente werden in Abhängigkeit von den auf ihnen gespeicherten Informationen datenschutzkonform gelöscht bzw. vernichtet.

4 Integrität

4.1 Erläuterung

Nach Art.32 Abs.1 lit.b) DSGVO sind geeignete technische und organisatorische Maßnahmen zu treffen, um die Integrität der Systeme und Dienste und damit die Unversehrtheit der Daten zu gewährleisten.

4.2 Eingabekontrolle

4.2.1 Erläuterung

Es muss nachträglich überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

4.2.2 Maßnahmen

Die Nachvollziehbarkeit von Eingabevorgängen wird über die restriktive Vergabe von Zugriffsrechten erreicht. Durch Beachtung des Minimalprinzips bei der Vergabe von Zugriffsrechten wird der Kreis zugriffsberechtigter Personen so klein wie möglich gehalten. Es ist gewährleistet, dass den Benutzern das Eingeben, Ändern oder Löschen von Daten nur entsprechend den für sie gültigen Berechtigungen möglich ist.

Die Aktivitäten des Administrators auf einem Server werden grundsätzlich protokolliert. Die Aufzeichnungen werden für definierte Zeiträume aufbewahrt.

Die Eingabe von personenbezogenen Daten für einen Kunden erfolgt durch DATAGROUP in der Regel nur im Rahmen der Benutzerregistrierung im Active Directory. Darüber hinaus kann es im Rahmen der allgemeinen administrativen Tätigkeiten zu einer Kenntnisnahme von personenbezogenen Daten kommen. Daher werden alle ausgeführten Tätigkeiten mit Hilfe eines ITSM-Tools und über korrespondierende Tickets dokumentiert und können nachvollzogen werden.

Grundsätzlich werden Aufträge eines Kunden über definierte Schnittstellen entgegengenommen und durch ein ITSM-Tool erfasst. Die weitere Bearbeitung wird zu jedem einzelnen Ticket dokumentiert.

Auf Kundenanforderung werden Zugriffe auf besonders schützenswerte Daten protokolliert.

Die Systemaktivität wird über das Ereignisprotokoll des verwendeten Betriebssystems aufgezeichnet.

Protokolldateien werden grundsätzlich in geschützten Systemverzeichnissen gespeichert, gegen Manipulation geschützt und entsprechend dem jeweils geltenden Datensicherungskonzept gesichert.

5 Pseudonymisierung und Verschlüsselung

5.1 Erläuterung

Art.25 Abs.1 sowie Art.32 Abs.1 lit.a) DSGVO verlangen, dass personenbezogene Daten möglichst pseudonymisiert und verschlüsselt verarbeitet werden. Pseudonymisiert bedeutet, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen (Art.4 Nr.5 DSGVO).

5.2 Maßnahmen

Auf Kundenanforderung werden personenbezogene Daten auf Entwicklungs- und Testsystemen im Rahmen der technischen Möglichkeiten anonymisiert oder pseudonymisiert.

Der Zugriff auf das Unternehmensnetzwerk von außen ist nur unter Verwendung gesicherter, verschlüsselter Verbindungen erlaubt (IPSec, L2TP oder SSL).

Datenträger, auf denen vertrauliche oder streng vertrauliche Daten gespeichert sind, werden verschlüsselt.

6 Verfügbarkeit und Belastbarkeit

6.1 Erläuterung

Nach Art.32 Abs.1 lit.b) DSGVO sind die Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung sicherzustellen. Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind. Nach Art.32 Abs.1 lit.c) DSGVO ist zudem sicherzustellen, dass personenbezogene Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können. Systeme müssen stets wie vorgesehen genutzt werden können und auch bei starker Auslastung ordnungsgemäß funktionieren.

6.2 Maßnahmen

Für die DATAGROUP Rechenzentren sind folgende Maßnahmen getroffen:

- Die Infrastruktur der Rechenzentren ist auf eine angemessene Verfügbarkeit der Systeme ausgelegt.
- Die Internetanbindung ist redundant und situativ über verschiedene Provider realisiert.
- Die Energieversorgung erfolgt über zwei Wege.
- Es sind Dieselaggregate (Notstromaggregate) für die zusätzliche Stromversorgung vorhanden.
- Es erfolgen regelmäßige Blackout-Tests und ein regelmäßiger Test der Notstrom-Dieselgeneratoren.
- Es besteht eine unterbrechungsfreie Stromversorgung (USV).
- Alle Systeme werden redundant an PDUs (Power Distribution Systeme – Stromverteiler in Racks) angeschlossen oder die Systeme werden redundant bereitgestellt.
- Klimaanlagen und USVs sind redundant ausgelegt.
- Die Temperatur im Rechenzentrum wird laufend elektronisch überwacht.
- Schutz gegen Wassereinbrüche durch Wassermelder.
- Das Rechenzentrum ist mit einer Brandmeldeanlage sowie einer Löschanlage gesichert. Es erfolgt eine Alarmaufschaltung und Weiterleitung an die Feuerwehr.
- Die Infrastrukturkomponenten werden regelmäßig gewartet. Es existieren Wartungsprotokolle.
- Die IT-technische Verkabelung ist in eigenen Trassen ausgeführt. An den Übergängen von Brandabschnitten sind Brandabschottungen eingebaut.
- Systeme sind entsprechend der Verfügbarkeits- und Kontinuitätsanforderungen redundant ausgelegt.
- Es findet eine regelmäßige und kontrollierte Datensicherung in einem zweistufigen Modell statt. Die Rekonstruierbarkeit der Daten wird regelmäßig getestet.

- Backupdatenträger werden in einem gesonderten Brandabschnitt in einem gesicherten und zutrittsbeschränkten DG-RZ-Bereich oder in einem geeigneten Tresor gelagert.
- Auf allen Servern sind Virenscanner installiert und werden automatisch mehrmals täglich mit aktuellen Signaturupdates versehen.
- Auf der Firewall erfolgt zusätzlich eine Filterung von Spam-Mails und Viren.
- DATAGROUP betreibt ein zentrales SOC (Security Operation Center).
- Ein SIEM (Security Information and Event Management) System, EDR (Endpoint Detection and Response) Systeme, Kompromittierungsscanner und Intrusion Prevention Systeme zur Angriffserkennung sind im Einsatz.
- Alle Systeme werden regelmäßig gemäß dokumentiertem Patch-Zyklus (bei akuten Bedrohungen unverzüglich) mit aktualisierten Softwareupdates der jeweiligen Softwarelieferanten gepatcht.
- Sämtliche kritischen DATAGROUP Systeme werden in einem zentralen VMS (Vulnerability Management System) überwacht (für Kundensysteme optional).
- Um Systemfehler und Systemausfälle zu minimieren, sind die Betriebsprozesse und Managementstrukturen im Rechenzentrum ITIL-konform ausgestaltet.
- Es besteht ein definierter und dokumentierter Change-Management Prozess. Dieser Prozess stellt sicher, dass notwendige oder gewünschte Änderungen an der IT-Infrastruktur anhand eines standardisierten und kontrollierten Verfahrens erfolgen.
- Ein Notfallmanagement in Anlehnung an BSI 200-4 oder ISO 22301 mit dem Ziel, einen unterbrechungsfreien Geschäftsbetrieb mit stetiger Wertschöpfung sicherzustellen, ist etabliert und dokumentiert.
- Sämtliche verwendete Hard- und Software wird über einen zentral gesteuerten Einkaufsprozess beschafft und ist in einem Inventar verzeichnet.
- Innerhalb der DATAGROUP Unternehmensgruppe ist durch ein Meldesystem sichergestellt, dass sicherheits- und datenschutzrelevante Vorfälle vorschriftsmäßig erfasst und bearbeitet werden.

7 Regelmäßige Überprüfung, Bewertung und Evaluierung

7.1 Erläuterung

Gemäß Art.32 Abs.1 lit.d) DSGVO ist ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu etablieren.

7.2 Maßnahmen

Innerhalb der DATAGROUP Unternehmensgruppe finden regelmäßig interne und externe Auditierungen statt.

Sicherheits- und datenschutzrelevante Vorfälle werden in einem monatlichen Company Security Report ausgewertet und an das Management berichtet.

DATAGROUP hat einen externen Dienstleister mit einem „Security Intelligence Service“ beauftragt, der die aus dem Internet erreichbaren Systeme kontinuierlich einer Sicherheitsprüfung aus der Perspektive eines realen Angreifers unterzieht.

DATAGROUP verfügt über ein professionelles IT-Service-Management. Dieses ist nach ISO/IEC 20000 zertifiziert.

Die Rechenzentren der DATAGROUP sind nach ISO/IEC 27001 bzw. DIN EN 50600 (RZ Ibbenbüren) zertifiziert.

Die Betriebsprozesse innerhalb der Rechenzentren sind einschließlich der dazugehörigen Verantwortlichkeiten konkret festgelegt und werden bei Vor-Ort-Audits vorgelegt.

8 Weisungsgemäße Verarbeitung

8.1 Erläuterung

Nach Art.28 Abs.3 S.2 lit.a) DSGVO ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den dokumentierten Weisungen des Auftraggebers verarbeitet werden. Ferner ist nach Art.32 Abs.4 DSGVO dafür Sorge zu tragen, dass Mitarbeiter, die Zugang zu personenbezogenen Daten haben, diese nur entsprechend den Weisungen des Verantwortlichen verarbeiten.

8.2 Auftragskontrolle

Externe Dienstleister, die für DATAGROUP Auftragsverarbeitungen durchführen, werden vertraglich gemäß Art.28 Abs.3 DSGVO verpflichtet und die Einhaltung der darin enthaltenen Verpflichtungen - insbesondere den technischen und organisatorischen Maßnahmen - in regelmäßigen Abständen kontrolliert.

Nach Durchführung eines Auftrags werden die durch den externen Dienstleister erbrachten Leistungen von dem verantwortlichen DATAGROUP Mitarbeiter auf Ordnungsmäßigkeit geprüft und abgenommen.

8.3 Beschäftigte der DATAGROUP

- Alle Beschäftigten sind schriftlich auf die Vertraulichkeit der Datenverarbeitung und zur Einhaltung des Datenschutzes im Unternehmen und darüber hinaus arbeitsvertraglich zum vertraulichen Umgang mit Betriebs- und Geschäftsgeheimnissen verpflichtet.
- Alle Beschäftigten werden im Zusammenhang mit der Verpflichtung auf die Vertraulichkeit der Datenverarbeitung und der Einhaltung des Datenschutzes im Unternehmen über die Themen Datenschutz und Informationssicherheit informiert.
- Um die Beschäftigten für die Themen Informationssicherheit und Datenschutz zu sensibilisieren und die Verfügbarkeit, Vertraulichkeit und Integrität von personenbezogenen Daten und sonstigen schützenswerten Informationen zu gewährleisten, ist innerhalb der DATAGROUP-Unternehmensgruppe ein Paket von Sicherheitsrichtlinien umgesetzt. Die Richtlinien werden regelmäßig überprüft und dem Stand der Technik und den organisatorischen Möglichkeiten angepasst. Soweit technisch möglich, werden die Vorgaben der Sicherheitsrichtlinien über Einstellungen systemseitig erzwungen.
- Ergänzend finden regelmäßig/wiederkehrend Schulungen (insbesondere mittels DATAGROUP Trainingsplattform) zu den in den Sicherheitsrichtlinien geregelten Themen und zum Datenschutz statt, um die Beschäftigten zu sensibilisieren und auf die sich daraus ergebenden Anforderungen im Unternehmen hinzuweisen.

9 Mobiles Arbeiten

Alle genannten TOM gelten - soweit anwendbar - auch für das mobile Arbeiten.

Die Mitarbeiter werden bzgl. der besonderen Herausforderungen des mobilen Arbeitens sowohl über Schulungen als auch das interne Anweisungs-Wesen regelmäßig sensibilisiert und sind auf die Einhaltung der DATAGROUP Richtlinie Mobilgeräte und mobiles Arbeiten verpflichtet.

Folgende TOM wurden mit Blick auf das mobile Arbeiten ergriffen:

- Zentrale Verwaltung der mobilen Endgeräte
- Vorgaben zum Schutz vor unbefugtem Einblick und Mithören
- Vorgaben zum Dokumentenhandling und zur sachgerechten Vernichtung von Dokumenten
- Verbot der Nutzung privater Speichermedien
- Vorgaben zur System-Härtung (auch der privaten Umgebung)
- Vorgaben zur zugriffssicheren Verwahrung von IT Equipment

Eine Kontrolle zur Einhaltung der Vorgaben zum mobilen Arbeiten findet in Form von Überprüfungen zur Teilnahme an Schulungen/Unterweisungen und verbindlichen Zusicherungen seitens der Beschäftigten statt.

Eine Kontrolle der privaten Räumlichkeiten der Beschäftigten findet - sofern erforderlich, rechtlich zulässig und unter Beachtung des Verhältnismäßigkeitsgrundsatzes - nur durch den Arbeitgeber und unter Einbindung notwendiger interner Stellen statt.

10 Kontaktdaten des Datenschutzbeauftragten

DATAGROUP hat für die unter Ziffer 2 genannten Unternehmen gemäß Art.37 Abs.4 S.1 DSGVO in Verbindung mit § 38 Abs.1 BDSG Dr. Christian Borchers als fachkundigen und unabhängigen betrieblichen Datenschutzbeauftragten bestellt.

Die Kontaktdaten lauten:

Dr. Christian Borchers

datenschutz süd GmbH

Telefon: 0931 304976-0

E-Mail: office@datenschutz-sued.de

Bei Fragen zum Datenschutz in der DATAGROUP-Unternehmensgruppe wenden Sie sich bitte direkt an:

Christian Dugall

datenschutz süd GmbH

Telefon: 0711 447086711

E-Mail: cdugall@datenschutz-sued.de