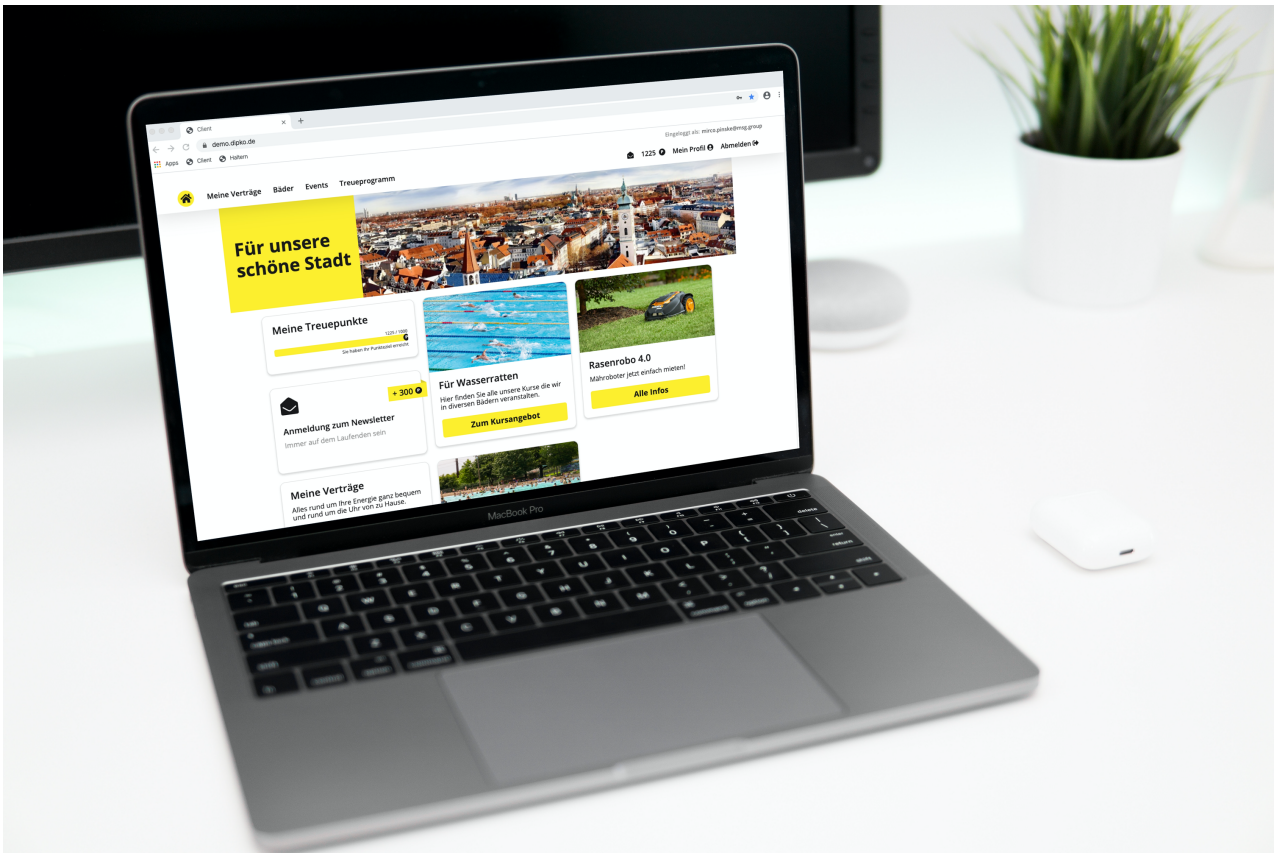

Technische und organisatorische Maßnahmen nach Art. 32 EU-DSGVO

Version 1.0

Digitalisierung fängt im Querverbund an

1 Inhaltsverzeichnis

1 Überblick

1.1 Ziel und Zweck

Dieses Dokument beschreibt die auf Seiten der DIPKO GmbH im Rahmen der Vereinbarung zur Auftragsdatenverarbeitung getroffenen technischen und organisatorischen Maßnahmen.

Nach Art. 28 Abs.3 c) i. V. m. Art. 32 Abs. 1 der EU-DSGVO ist der Auftragnehmer im Rahmen der Auftragsdatenverarbeitung unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Die in diesem Dokument beschriebenen technischen und organisatorischen Maßnahmen gemäß Artikel 32 der DSGVO sind als DIPKO GmbH Standard zu verstehen. Sie finden Anwendung zwischen den Parteien, sofern eine Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen wurde. Individuelle Ergänzungen und Detaillierungen im Rahmen der Auftragsverarbeitung sind in der jeweiligen Auftragsverarbeitungsvereinbarung festzulegen.

2 Technische und Organisatorische Maßnahmen

Die Geschäftsführung der DIPKO GmbH hat einen externen Datenschutzbeauftragten zur Wahrnehmung der Beratungs- und Kontrollfunktionen der EU-DSGVO und des BDSG (neu) eingesetzt.

Kontaktdaten:

Stephan Schuldt
Grimmaische Str. 2-4
04109 Leipzig
+49 341 231062-25
s.schuldt@gp-data.de

Die DIPKO GmbH hat zum Hosting der SaaS-Lösung „DIPKO“ die msg services ag beauftragt. Die TOM der msg services ag sind daher im Bereich Subunternehmen aufgelistet. Die msg services ag betreibt ein ISO 9001 zertifiziertes Qualitätsmanagement-System (QMS) und ein ISO 27001 zertifiziertes Informationssicherheitsmanagement-System (ISMS).

Im Rahmen des Datenschutzmanagement-Systems (DSMS) erfolgt die Umsetzung der Vorgaben aus der EU-DSGVO und dem BDSG (neu).

Die Mitarbeiter erhalten bei Beginn ihrer Tätigkeit eine Datenschutzunterweisung. Später erfolgt eine regelmäßige Sensibilisierung durch monatliche Newsletter, Schulungen und persönliche Ansprache. Durch interne und externe Audits erfolgt eine regelmäßige Überprüfung.

Die zertifizierten Rechenzentren der msg services ag befinden sich in Ismaning/München. Nachfolgend sind die Maßnahmen gemäß Art. 32 DSGVO beschrieben.

In den Büroräumlichkeiten der DIPKO GmbH werden keine Server betrieben. Zusätzlich setzt die DIPKO GmbH Dienste von Amazon Web Services ein, die durch die msg services ag gemanaged werden. Sämtliche Server stehen in einem von Amazon Web Services betriebenen Rechenzentrum in Frankfurt am Main (Deutschland).

2.1 Vertraulichkeit

2.1.1 Zutrittskontrolle

- Das Firmengebäude besitzt Sicherheitsschlösser
- Jedem Mitarbeiter der DIPKO GmbH wird ein Schlüssel für das Firmengebäude sowie ggf. ein Schlüssel zu seinem jeweiligen Büro ausgehändigt
- Die Vergabe von Schlüsseln wird dokumentiert und regelmäßig überprüft
- Besucher werden immer durch mindestens einen Mitarbeiter der DIPKO GmbH begleitet
- Sorgfältige Auswahl von Dienstleistern

2.1.2 Zugangskontrolle

- Die Vergabe und Verwaltung von Benutzerrechten für einzelne Systeme erfolgt ausschließlich durch Systemadministratoren
- Alle Arbeitsgeräte, auf denen personenbezogene Daten verarbeitet werden, sind für den jeweiligen Mitarbeiter personalisiert, mit einem Passwort geschützt und verwenden das aktuelle Betriebssystem
- Clean-Desk-Policy
- Für die Verwendung eines sicheren Passwortes gelten folgende Regelungen: - muss mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen und eine Zahl enthalten, sowie mindestens 8 Zeichen lang sein
- Mitarbeiter sind angewiesen den Arbeitsplatz bei Verlassen zu sperren.
- Einsatz einer aktuellen Virenschutzsoftware

2.1.3 Zugriffskontrolle

- Definierte Benutzergruppen
- Protokollierung des Zugriffs auf personenbezogene Daten (Lesen, Ändern, Löschen)
- Logins werden nicht geteilt, jedem Nutzer ist ein Login zugeordnet
- Trennung von Systemdateien unterschiedlicher Anwendungen
- Trennung von Benutzerdateien verschiedener Benutzer

2.1.4 Trennungskontrolle

- Maßnahmen der physikalischen Trennung der Daten vorhanden/Speicherung in getrennten Datenbanken
- Trennung von Testdaten/Entwicklungsdaten und Produktivdaten
- Maßnahmen der logischen Trennung der Daten
- Zugriffsberechtigungen nach funktioneller Zuständigkeit

2.2 Integrität

2.2.1 Weitergabekontrolle

- Verschlüsselung von Speichermedien
- Gesicherter File Transfer (z.B. sftp)
- Gesicherter Datentransport (z.B. SSL, ftp, ftps, TLS)
- Mehrstufiges Virenkonzept
- Datenschutzkonforme Entsorgung elektronischer Datenträger
- Datenschutzkonforme Vernichtung von Papierdokumenten

2.2.2 Eingabekontrolle

- Berechtigungskonzept
- Löschkonzept
- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Protokollierung (betroffener Datensatz, Zeitpunkt der Eingabe, ausführender Benutzeraccount, Aktivität (Neuanlage, Veränderung, Löschung)

2.3 Verfügbarkeit und Belastbarkeit

2.3.1 Verfügbarkeitskontrolle

- Anti-Viren-Software
- Regelmäßige Updates der eingesetzten Software
- Redundanz der Hardware
- Diebstahlsicherung von Datenverarbeitungsanlagen

2.3.2 Rasche Wiederherstellbarkeit

- Backup & Recovery-Konzept
- Regelmäßige Tests der Datenwiederherstellung

2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

2.4.1 Datenschutzmanagement

- Datenschutz-Richtlinie
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Führen einer Übersicht über die Verarbeitungstätigkeiten

2.4.2 Incident-Response-Management

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO) ist vorhanden
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO) ist vorhanden

2.4.3 Auftragskontrolle

- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

2.5 Technische und Organisatorische Maßnahmen der Subunternehmen: Amazon Web Services

2.5.1 Überblick

Die über die Plattform DIPKO erhobenen Daten werden auf der IT-Infrastruktur der Amazon Web Services Inc., 410 Terry Avenue North, Seattle WA 98109 - nachfolgend „AWS" genannt – in der AWS Verfügbarkeitszone „Frankfurt/Deutschland" gespeichert. AWS garantiert, die Daten nicht außerhalb der Verfügbarkeitszone zu transferieren (https://aws.amazon.com/de/compliance/germany-data-protection/).

Wir haben bei der Auswahl unseres Rechenzentrumbetreibers auf größtmögliche Sicherheit geachtet. AWS verfügt über international anerkannte Zertifizierungen, die von unabhängigen renommierten Beratungsgesellschaften attestiert wurden und die Erfüllung höchster Sicherheitsanforderungen nachweisen.

AWS weist insbesondere folgende internationale Zertifizierungen auf:

- ISO 9001, Weltweiter Qualitätsstandard
- ISO 27001, Sicherheitsmanagementkontrollen
- ISO 27017, Cloud-spezifische Kontrollen
- ISO 27018, Schutz personenbezogener Daten

Darüber hinaus hat AWS im November 2016 als erster Cloud-Service-Anbieter in Deutschland vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ein C5-Testat für Cloud-Anwendungen erlangt.

2.5.2 Vertraulichkeit

2.5.2.1 Zutrittskontrolle

AWS hat die folgenden technischen und organisatorischen Maßnahmen umgesetzt, die die AWS Einrichtungen vor unbefugtem physischem Zutritt schützen. Derzeit umfassen diese Maßnahmen unter anderem:

- Die AWS Rechenzentren, Server, Netzwerkausstattung und Hostsoftwaresysteme (physische Bestandteile des AWS Netzwerks) sind in unscheinbaren Gebäuden untergebracht.
- Die AWS Gebäude sind durch physische Sicherheitsmaßnahmen geschützt, um den unberechtigten Zutritt weiträumig (z.B. Zaun, Wände) als auch in den Gebäuden selbst zu verhindern.
- Der Zutritt zu Serverstandorten wird mit elektronischen Zugangskontrollen verwaltet und durch Alarmanlagen gesichert, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird.
- Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiter- oder Lieferantendatensatz deaktiviert wurde.
- Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet.
- Der Zutritt zu sensiblen Bereichen wird durch Videoüberwachung überwacht.
- Ausgebildete Sicherheitskräfte bewachen die AWS-Rechenzentren und die unmittelbare Umgebung davon 24 Stunden am Tag, 7 Tage die Woche.

2.5.2.2 Zugangskontrolle

AWS hat die folgenden technischen und organisatorischen Maßnahmen umgesetzt, die das AWS-Netzwerk vor unbefugtem Zugang schützen. Derzeit umfassen diese Maßnahmen unter anderem:

- Der Benutzer- und Administratorzugriff auf das AWS-Netzwerk beruhen auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können.
- Der Benutzerzugriff auf das AWS-Netzwerk wird erst aktiviert, wenn die Personalabteilung einen entsprechenden Datensatz im HR-System erstellt hat.
- Bei AWS gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus muss eine entsprechende Berechtigung vorliegen.
- Die erteilten Zugriffsrechte auf AWS IT-Systeme werden mindestens vierteljährlich von zuständigen Mitarbeitern überprüft. Zugriffsberechtigungen werden sofort aufgehoben, wenn die entsprechenden Zugriffsrechte für die Tätigkeiten des Benutzers nicht mehr erforderlich sind.
- Die Zugriffsrechte auf das AWS IT-System werden innerhalb von 24 Stunden nach Deaktivierung des jeweiligen Mitarbeiterdatensatzes im HR-System durch die Personalabteilung aufgehoben.
- Passwörter/Pass-Phrasen für die Erstanmeldung bestehen aus einem einmaligen Wert und werden nach der ersten Verwendung sofort geändert.

- Benutzerpasswörter/-Pass-Phrasen werden spätestens alle 90 Tage geändert. Es sind nur komplexe Passwörter zulässig. Die Änderung des Passworts durch einfache Passwortvariationen z. B. durch Ändern einer einzigen Stelle, ist nicht möglich.
- Das Erstellen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsmerkmalen wird zusammen mit einem Zeitstempel protokolliert.
- Auf Amazon Equipment (z. B. Notebooks) ist Antivirus-Software installiert, die einen E-Mail-Filter sowie eine Malware-Erkennung enthält.
- AWS Firewall Geräte sind so konfiguriert, dass sie den Zugriff auf die Datenverarbeitungsumgebung beschränken und die Absicherung der Computing-Cluster verstärken.
- AWS Firewall-Richtlinien (d.h. Konfigurationsdateien) werden automatisch alle 24 Stunden an die Firewall-Geräte übertragen und aufgespielt.
- Die Kommunikation im AWS-Netzwerk erfolgt SSH-Verschlüsselt („Public key“) durch einen Bastion-Host, der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten beschränkt und alle Aktivitäten im AWS-Netzwerk für eine Sicherheitsüberprüfung protokolliert.

Darüber hinaus hat die DIPKO GmbH die folgenden technischen und organisatorischen Maßnahmen ergriffen um einen unbefugten Zugriff auf die von der DIPKO GmbH auf dem AWS-Netzwerk gespeicherten Daten vor einem unbefugten Zugang zu schützen:

- Der Zugriff auf das AWS-Netzwerk erfolgt über eine verschlüsselte Verbindung und ist ausschließlich Mitarbeitern der DIPKO GmbH vorenthalten.
- Der Zugriff auf die Daten und Dienste des AWS-Netzwerks wird über eine differenzierte Zugriffsregelung geregelt.

2.5.2.3 Zugriffskontrolle

AWS hat die folgenden technischen und organisatorischen Maßnahmen zur Einräumung und Regelung von Zugriffsrechten für Mitarbeiter von AWS umgesetzt. Derzeit umfassen diese Maßnahmen unter anderem:

- Benutzer und Administratorzugriff auf das AWS-Netzwerk beruhen auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können.
- Bei AWS gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen.
- Die erteilten Zugriffsrechte auf AWS IT-Systeme werden mindestens vierteljährlich von zuständigen Mitarbeitern überprüft.

- Das Erstellen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsmerkmalen wird zusammen mit einem Zeitstempel protokolliert.

Darüber hinaus hat die DIPKO GmbH die folgenden technischen und organisatorischen Maßnahmen ergriffen, um zu gewährleisten, dass Mitarbeiter der DIPKO GmbH ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können:

- Rollen- und Rechtekonzept
- Identitätsmanagementsystem
- Regelmäßiges Überprüfen des Rollen- und Rechtekonzepts

2.5.2.4 Trennungskontrolle

AWS hat die folgenden technischen und organisatorischen Maßnahmen getroffen, um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennte verarbeitet werden:

- Die AWS-Umgebung ist eine virtualisierte Mehrmandantenumgebung. AWS hat Prozesse zur Sicherheitsverwaltung sowie Sicherheitskontrollen eingerichtet, die die Trennung von Daten einzelner Kunden ermöglicht. AWS-Systeme sind so konzipiert, dass Kunden nicht auf physisch Hosts oder Instanzen zugreifen können, die nicht zu ihrem AWS-Account gehören. Dies wird durch die Filterung im Rahmen einer Virtualisierungssoftware ermöglicht.

2.5.3 Integrität

2.5.3.1 Weitergabekontrolle

AWS hat die folgenden technischen und organisatorischen Maßnahmen umgesetzt, um sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Derzeit umfassen diese Maßnahmen unter anderem:

- Die von AWS ergriffenen Maßnahmen zur Verhinderung von unbefugtem Kopieren der physischen Speicherinfrastruktur als solche (z. B. Kopieren der Daten des Kunden durch Übertragung auf ein externes Speichermedium wie eine Festplatte) sind in den Maßnahmen wie oben in Ziffern 1.1–1.3 beschrieben enthalten. Darüber hinaus dürfen AWS Mitarbeiter und freie Mitarbeiter keine privaten elektronischen Geräte und mobile Datenträger an AWS-Informationssysteme anschließen.
- Nutzung eines rollenbasierten Zugriffsberechtigungsmodells
- Firewall-Richtlinien
- Implementierung eines Vorfallreaktionsplans

- Wenn die Lebensdauer eines Speichergerätes zu Ende geht, führt AWS einen speziellen Prozess zur Außerbetriebnahme durch, damit Kundeninhalte nicht an unbefugte Personen gelangen. Alle stillgelegten Magnetspeichergeräte werden entmagnetisiert und den branchenüblichen Vorgehensweisen und dem geltenden Datenschutzgesetz entsprechend physisch zerstört.
- AWS-Mitarbeiter greifen SSH-Verschlüsselt („Public key“) durch einen Bastion-Host auf das AWS-Netzwerk zu. Der Bastion-Host beschränkt den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten.

Die DIPKO GmbH hat darüber hinaus folgende Maßnahmen ergriffen um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung auf das AWS-Netzwerk nicht unbefugt gelesen werden können:

- Die Verbindungen zu dem AWS-Netzwerk erfolgen über HTTP oder HTTPS. TTP oder HTTPS sind Verschlüsselungsprotokolle, die zum Schutz vor Abhörangriffen, Datenmanipulation oder Fälschung von Nachrichten entwickelt wurde.

2.5.3.2 Eingabekontrolle

AWS hat die folgenden technischen und organisatorischen Maßnahmen umgesetzt, die es ermöglichen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogenen Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- AWS-Entwickler und Administratoren, die zur Wartung der AWS-Services Zugriff auf das AWS-Netzwerk benötigen, müssen ausdrücklich Zugriff auf die entsprechenden Komponenten beantragen. Berechtigte AWS-Mitarbeiter greifen SSH-verschlüsselt („Public key“) durch einen Bastion-Host auf das AWS Netzwerk zu. Der Bastion-Host beschränkt den Zugriff auf Netzwerkgeräte und andere Komponenten und protokolliert alle Aktivitäten zur Sicherheitsüberprüfung.
- AWS hat für alle System und Geräte innerhalb des AWS-Netzwerks Ereigniskategorien festgelegt, die sich durch Audits überprüfen lassen. Service-Teams konfigurieren die Auditfunktionen um sicherheitsrelevante Ereignisse zur protokollieren. Die Auditdaten enthalten eine Gruppe von Datenelementen („Wann“ (Zeitstempel), „Wo“ (Quelle), „Wer“ (Benutzername), „Was“ (Inhalt)).

Die DIPKO GmbH hat darüber hinaus folgende Maßnahmen ergriffen um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten die auf dem AWS-Netzwerk gespeichert sind, eingegeben, verändert oder entfernt worden sind:

- Änderungen/Eingaben von personenbezogenen Daten werden protokolliert
- Zugriffe und Zugriffsversuche werden aufgezeichnet.

2.5.4 Verfügbarkeit und Belastbarkeit

AWS hat die folgenden technischen und organisatorischen Maßnahmen zum Schutz der Daten gegen zufällige Zerstörung oder Verlust umgesetzt. Derzeit umfassen diese Maßnahmen unter anderem:

- AWS hat Einrichtungen zur automatischen Branderkennung und –bekämpfung in den AWS-Rechenzentren installiert. Das Branderkennungssystem setzt Rauchsensoren in der gesamten Umgebung der Rechenzentren, in mechanischen und elektrischen Bereichen der Infrastruktur, Kühlräumen und in den Räumen, in denen die Generatoren untergebracht sind, ein.
- Die elektrischen Anlagen der Rechenzentren wurden so entwickelt, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs gewartet werden können. Eine unterbrechungsfreie Stromversorgung sorgt im Fall eines Stromausfalls dafür, dass kritische Bereiche der Anlage weiterhin mit Strom versorgt werden. Die Rechenzentren verfügen darüber hinaus über Generatoren, die die gesamte Anlage mit Notstrom versorgen können.
- Mitarbeiter und entsprechende Systeme überwachen und steuern die Temperatur und Luftfeuchtigkeit innerhalb der Rechenzentren auf einem angemessenen Niveau.
- Es werden darüber hinaus vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.

2.6 Technische und Organisatorische Maßnahmen der Subunternehmen: msg services ag

2.6.1 Vertraulichkeit

2.6.1.1 Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren:

- Die Gebäude sind mit Sicherheitsschließanlagen bzw. elektronischen Zutrittskontrollsystemen ausgerüstet. Definierte Büroräume besitzen zusätzlich elektronische Türschlösser (SimonsVoss)
- Der Zutritt zu den Rechenzentren erfolgt mittels elektronischer Zutrittskontrollsysteme (Multi-Faktor), Zutrittsberechtigung haben nur autorisierte Mitarbeiter. Die entsprechenden Zutrittsberechtigungen werden regelmäßig überprüft
- Arbeitsanweisung zur Handhabung von Zutrittskontrollen
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- Sicherung durch Wachdienst mit regelmäßigen Kontrollgängen
- Abhängig vom Standort: Einsatz von Alarmanlagen und datenschutzkonforme Videoüberwachung in sicherheitskritischen Bereichen

2.6.1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Organisatorische und technische Regelung zum sicheren und ordnungsgemäßen Einsatz von Passwörtern
- Serversysteme sind nur mit Konsolenpasswort oder über passwortgeschützte und verschlüsselte Verbindungen administrierbar
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine unpersönlichen Sammelkonten („AZUBI1“)
- Festplatten- und Datenträgerverschlüsselung
- Einsatz von mehrstufigen Schutzmechanismen (Multi-Vendor Virenscanner, Multi-Vendor Firewalls)
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (Virenscanner, Microsoft Patches)
- Richtlinie zum physikalischen Schutz benutzter Systeme (Bildschirmsperre, Blickschutzfilter)
- Logische Zugangsregelung zum Netzwerk, Netzwerkzugang erhalten nur freigegebene Unternehmensgeräte (zertifikatsbasierte Network Access Control-Lösung)

2.6.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Clean Desk Policy
- Benutzeridentifizierung und Berechtigungsvergabeverfahren (Identity Management)

- Trennung von Berechtigungsbewilligung (organisatorisch) durch den Verantwortlichen sowie Berechtigungsvergabe (technisch) durch die IT
- Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(-gruppen)
- Netzwerksegmentierung, Netzzonen, Firewalls
- Richtlinie zum Patchlevel eingesetzter Systeme (Client Security Policy)

2.6.1.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Logische bzw. physikalische Mandantentrennung
- Die Daten des Auftraggebers und anderer Mandanten werden, soweit möglich, von unterschiedlichen Mitarbeitern des Auftragnehmers verarbeitet
- Generelle Trennung von Test- und Produktionsumgebungen

2.6.1.5 Pseudonymisierung

Bei der Pseudonymisierung handelt es sich um eine zentrale technische und organisatorische Sicherungsmaßnahme, die die DSGVO nicht nur in Art. 32 Abs. 1, sondern wiederholt in unterschiedlichem Zusammenhang erwähnt. Sie kann Einfluss auf die Zulässigkeit einer Verarbeitung personenbezogener Daten haben und erhöht den Schutz der Rechte und Freiheiten der Betroffenen. Der Erwägungsgrund 26 DSGVO stellt hierbei eindeutig heraus, dass auch pseudonymisierte Daten weiterhin personenbezogene Daten bleiben.

Grundsätzlich stehen drei Pseudonymisierungsmethoden zur Verfügung:

- Der Betroffene vergibt selbst ein Pseudonym und separiert dieses von den Daten, die ihn identifizieren.
- Ein unabhängiger Dritter, der über die entsprechende Zuordnungsregel verfügt, vergibt ein Pseudonym für den Betroffenen (§ 7 Abs. 1 Signaturgesetz (SigG)).
- Die Verantwortliche Stelle erstellt ein Pseudonym und separiert dieses von den identifizierenden

Merkmalen des Betroffenen. Da die datenverarbeitende Stelle selbst über die Zuordnungsregel verfügt, bietet eine derartige Pseudonymisierung nur Schutz gegenüber Dritten. Das Vorgehen ist in Erwägungsgrund 29 als technische und organisatorische Sicherungsmaßnahme vorgesehen.

Die Entscheidung über die Pseudonymisierungsmethode hängt vom jeweiligen Anwendungsfall ab. Im Rahmen einer Auftragsverarbeitung erfolgt die Pseudonymisierung durch die Verantwortliche Stelle, so dass dem Auftragsverarbeiter die Identifikation der betroffenen Person ohne die Hilfe der Verantwortlichen Stelle nicht möglich ist.

2.6.2 Integrität

2.6.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger 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:

- Sicherung elektronischer Übertragung mittels verschlüsselter Verbindungen (VPN, TLS)
- Sicherung bei der Übermittlung (Verfahrensbeschreibung, Protokollierung)
- Sicherung beim physikalischen Transport (Verschlüsselung des Datenträgers, Einsatz eines Kuriers)
- Dokumentierte Datenträgervernichtung nach DIN 66399 für vertrauliche und streng vertrauliche Daten

2.6.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Nur die im Zusammenhang mit Leistungen aus dem Vertrag tätigen Mitarbeiter des Auftragnehmers sind zur Verarbeitung personenbezogener Daten des Auftraggebers ermächtigt
- Benutzerauthentifizierung der zur Eingabe, Änderung oder Löschung autorisierter Personen
- Berechtigungssteuerung der Zugriffsart (lesender oder schreibender Zugriff)
- Protokollierung der Zugriffe

2.6.3 Verfügbarkeit und Belastbarkeit

2.6.3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Backup- und Recovery-Konzept mit täglicher Sicherung und Aufbewahrung der Datenträger in getrennten Brandabschnitten / Rechenzentren
- Verfahren zur Wiederherstellung von Daten aus Backup (z. B. Restore nur nach autorisiertem Auftrag)
- Einsatz von Schutzprogrammen (Virenscanner, Firewalls)
- Einsatz von Festplattenspiegelung im Server- und Storagebereich (RAID)
- Einsatz unterbrechungsfreier Stromversorgung im Serverbereich (USV, NEA)
- Einsatz von Klimatisierung und Brandschutz (Brandfrüherkennung, Löschanlage)
- Incident- / Notfall Management und Disaster Recovery Verfahren
- Durch Security Policy vorgeschriebener Diebstahlschutz

2.6.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

2.6.4.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Der jeweilige Vertrag mit dem Auftraggeber enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers und benennt die Weisungsbefugnisse
- Definierte verantwortliche Ansprechpartner auf Seiten des Auftraggebers

- Der Vertrag enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Auftragnehmer außerhalb des schriftlich formulierten Auftrags
- Der Auftragnehmer hat einen externen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse
- Dokumentation der IT-Servicemanagement-Aktivitäten (CMDB und Ticketsystem)

2.6.4.2 Datenschutz-Management

Ein Datenschutz-Management-System gewährleistet, dass die Rechenschaftspflicht zum Nachweis der Einhaltung der gesetzlichen Grundsätze und Regelungen, des Stands der Technik und der Aktualität und Wirksamkeit der Maßnahmen eingehalten wird. Folgende Maßnahmen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Datenschutzorganisation mit benanntem Beauftragten für den Datenschutz
- Richtlinien und Anweisungen zur Gewährleistung der Datenschutz Compliance
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter zum Datenschutz
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO) als Verantwortliche Stelle und Auftragsverarbeiter
- Prozesse zur Wahrung der Betroffenenrechte

2.6.4.3 Incident-Response-Management

Erkannte oder vermutete Sicherheitsvorfälle werden im Rahmen des Incident Management erfasst. Das Informationssicherheitsmanagement-System (ISMS) ist hierzu mit dem Datenschutzmanagement-System (DSMS) gekoppelt. Im Rahmen des DSMS gewährleistet ein Prozess, dass im Fall von Datenschutz- verstößen ein Meldeprozess ausgelöst wird.

- Meldeprozess für Datenschutzverletzungen nach Art. 28 DSGVO gegenüber der Verantwortlichen Stelle im Rahmen einer Auftragsverarbeitung
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

2.6.4.4 Datenschutzfreundliche Voreinstellungen

Durch geeignete technische und organisatorische Maßnahmen wird gewährleistet, dass in Bezug auf die Menge, den Umfang, der Speicherfrist und der Zugänglichkeit durch Voreinstellungen die Verarbeitung nur für den jeweiligen bestimmten Verarbeitungszweck erfolgt.

Die Default-Einstellungen werden sowohl bei den standardisierten Voreinstellungen von Systemen und Applikationen als auch bei der Einrichtung der Datenverarbeitungsverfahren von Seiten msg services berücksichtigt.

Art und Umfang des Personenbezugs sowie angemessene Pseudonymisierung und Anonymisierung werden im Rahmen der Projektinitialisierung berücksichtigt.