VEREINBARUNG ÜBER DIE AUFTRAGSDATENVERARBEITUNG (ART 28 DSGVO) FÜR STREAMDIVER CLOUD SERVICES

(„AUFTRAGSVERARBEITERVEREINBARUNG“ ODER „AVV“)

Diese Auftragsverarbeitervereinbarung wird in Vereinbarungen zwischen Streamdiver GmbH (nachfolgend „SD“ genannt) und Dritten („Auftraggeber“) betreffend die Erbringung von Cloud Services einschließlich Support einbezogen und regelt in diesem Verhältnis die Verarbeitung Personenbezogener Daten durch SD im Auftrag des Auftraggebers.

1 DEFINITIONEN

Auftragsverarbeiter	bezeichnet eine natürliche oder justische Person, öffentliche Behörde, Einrichtung oder andere Stelle, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, sei es direkt als Auftragsverarbeiter eines Verantwortlichen oder indirekt als Unterauftragsverarbeiter eines Auftragsverarbeiters, der Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Auftraggeberdaten	bezeichnet alle Inhalte, Materialien, Daten, personenbezogene Daten und Informationen, die von Autorisierten Nutzern im Produktivsystem eines Cloud Service erfasst, bearbeitet und verwaltet werden.
Autorisierter Nutzer	(oder „Named User“) bezeichnet eine Person, die im Unternehmen des Auftraggebers oder bei Geschäftspartnern des Auftraggebers tätig ist und der der Auftraggeber eine Zugriffsberechtigung für den Cloud Service erteilt hat.
Bestellung	oder „Vereinbarung“ bezeichnet eine Vereinbarung zwischen SD und dem Auftraggeber auf Basis eines von SD gelegten Angebots und einer mit dem Angebotsinhalt übereinstimmenden Angebotsannahme über Cloud Services, die auf die vorliegenden Nutzungsbedingungen (und allfällige weitere Dokumente) Bezug nimmt.
Betroffene Person	bezeichnet eine identifizierte oder identifizierbare natürliche Person gemäß der Definition im Datenschutzrecht.
Cloud Service	bezeichnet jede spezifische von SD unter einer Bestellung bereitgestellte On-Demand-Lösung (einschließlich Support).
Datenschutzrecht	bezeichnet die geltenden Rechtsvorschriften zum Schutz der Grundrechte und Freiheiten von Personen und deren Persönlichkeitsrecht in Bezug auf die Verarbeitung von Personenbezogenen Daten im Rahmen der Vereinbarung (und beinhaltet in Bezug auf die Beziehung zwischen den Parteien bezüglich der Verarbeitung Personenbezogener Daten durch SD im Auftrag des Auftraggebers, die DSGVO als Mindeststandard, unabhängig davon, ob die Personenbezogenen Daten der DSGVO unterliegen oder nicht.).
EU-Standardvertragsklauseln	(auch als „EU-Modellklauseln“ bezeichnet) bezeichnet die Standardvertragsklauseln (Auftragsverarbeiter) bzw. jegliche nachfolgenden von der Europäischen Kommission veröffentlichten Versionen dieser Klauseln (die automatisch gelten).
EWR	bezeichnet den Europäischen Wirtschaftsraum, das sind die Mitgliedsstaaten der EU sowie Island, Liechtenstein und Norwegen.
Personenbezogene Daten	bezeichnet alle Informationen in Bezug auf eine Betroffene Person, die dem Schutz des Datenschutzrechts unterliegen. In diesem AVV sind darunter nur diejenigen personenbezogenen Daten zu verstehen, die (i) vom Auftraggeber oder dessen Autorisierten Nutzern im Cloud Service oder durch dessen Nutzung erfasst werden oder (ii) von SD oder ihren Unterauftragsverarbeitern bereitgestellt werden oder auf die SD oder ihre Unterauftragsverarbeiter zugreifen, um den Support gemäß der Vereinbarung zu leisten. Personenbezogene Daten sind eine Teilmenge der Auftraggeberdaten.
Unterauftragsverarbeiter	bezeichnet verbundene Unternehmen der SD sowie Dritte, die von SD zur Erbringung des Cloud Service eingesetzt werden, und die Personenbezogene Daten gemäß dieser AVV verarbeiten.
Verantwortlicher	bezeichnet die natürliche oder juristische Person, öffentliche Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung Personenbezogener Daten bestimmt; für die Zwecke dieses AVV gilt der Verantwortliche im Verhältnis zu SD, wenn der Kunde der SD als Auftragsverarbeiter für einen anderen Verantwortlichen handelt, als zusätzlicher und unabhängiger Verantwortlicher mit den entsprechenden Rechten und Pflichten eines Verantwortlichen gemäß diesem AVV.

2 GEGENSTAND DER VEREINBARUNG

2.1 Gegenstand des an SD erteilten Auftrages ist die Erbringung von IT-Service-Leistungen auf Basis und im Rahmen der Bestellung.

2.2 SD und Auftraggeber sind jeweils eigenverantwortlich verpflichtet, die Anforderungen, die nach geltendem Datenschutzrecht an Verantwortliche und Auftragsverarbeiter gestellt werden, zu überprüfen und umzusetzen.

2.3 SD wird als Auftragsverarbeiter tätig und der Auftraggeber, bzw. die Rechtspersonen, denen der Auftraggeber die Nutzung des Cloud Service gestattet, handeln als Verantwortliche im Rahmen des AVV. Der Auftraggeber ist einziger Kontaktpunkt und allein verantwortlich für die Einholung aller relevanten Genehmigungen, Zustimmungen und Einwilligungen für die Verarbeitung Personenbezogener Daten gemäß diesem AVV. Soweit vom Auftraggeber Genehmigungen, Zustimmungen, Weisungen oder Einwilligungen erteilt werden, werden diese nicht nur im Namen des Auftraggebers, sondern auch im Namen allfälliger anderer Verantwortlicher, die den Cloud Service nutzen, erteilt. Wenn SD den Auftraggeber informiert oder ihm Meldungen übermittelt, gelten diese Informationen oder Meldungen als von denjenigen Verantwortlichen erhalten, denen der Auftraggeber die Nutzung des Cloud Service gestattet hat. Es liegt in der Verantwortung des Auftraggebers, diese Informationen und Meldungen an die entsprechenden Verantwortlichen weiterzuleiten.

2.4 Jede Partei ist für die Einhaltung ihrer Dokumentationspflichten verantwortlich, insbesondere für die Führung von Verarbeitungsverzeichnissen, soweit dies nach dem Datenschutzrecht erforderlich ist. Jede Partei unterstützt die andere Partei in angemessener Weise bei der Erfüllung von deren Dokumentationspflichten, einschließlich der Bereitstellung der Informationen, die die andere Partei von ihr benötigt, in einer von der anderen Partei in angemessener Weise angeforderten Form, damit die andere Partei den Verpflichtungen im Zusammenhang mit der Führung von Verarbeitungsverzeichnissen nachkommen kann.

3 VERARBEITUNG IM AUFTRAG

3.1 Im Rahmen der Erbringung des Cloud Service werden von SD üblicherweise Daten folgender Kategorien verarbeitet:

3.1.1. Name / Benutzername

3.1.2. E-Mail-Adresse

3.1.3. IP-Adresse

3.1.4. Rechte & Rollen - Gruppenzugehörigkeit/Systemzugriffs-/Nutzungs- und Berechtigungsdaten

3.2 Betroffene Personen sind Autorisierte Nutzer und somit typischerweise Mitarbeiter oder Geschäftspartner denen durch den Auftraggeber Zugriff auf das Cloud Service eingeräumt wird.

3.3 Die personenbezogenen Daten werden im Wesentlichen folgenden Verarbeitungsmaßnahmen unterzogen:

3.3.1. Verwendung von Personenbezogenen Daten, um den Cloud Service einzurichten, zu betreiben, zu überwachen und bereitzustellen (einschließlich operativen und technischen Supports)

3.3.2. Bereitstellung von Consulting Services

3.3.3. Kommunikation mit Autorisierten Nutzern

3.3.4. Speicherung von Personenbezogenen Daten in speziellen Rechenzentren (Multi-Tenant-Architektur)

3.3.5. Upload von Korrekturen oder Upgrades in den Cloud Service

3.3.6. Erstellen von Sicherungskopien der Personenbezogenen Daten

3.3.7. Rechnergestützte Verarbeitung von Personenbezogenen Daten, einschließlich Datenübertragung, Abruf von Daten, Zugang zu Daten

3.3.8. Netzwerkzugang, um die Übertragung von Personenbezogenen Daten zu ermöglichen

3.3.9. Ausführung von Anweisungen des Auftraggebers gemäß der Vereinbarung

4 PFLICHTEN DES AUFTRAGSVERARBEITERS

4.1 SD wird Personenbezogene Daten nur in Übereinstimmung mit den dokumentierten Weisungen des Auftraggebers verarbeiten. Die Vereinbarung (einschließlich dieses AVV) stellt eine solche dokumentierte Erst-Weisung dar, und jede Nutzung des Cloud Service stellt eine weitere Weisung dar. SD unternimmt alle zumutbaren Anstrengungen, um allen anderen Weisungen des Auftraggebers zu folgen, soweit sie nach Datenschutzrecht erforderlich, technisch durchführbar und ohne Änderungen am Cloud Service möglich sind. Sollte eine der vorgenannten Ausnahmen zu treffen oder SD anderweitig einer Weisung nicht nachkommen können oder der Meinung sein, dass eine Weisung gegen das Datenschutzrecht verstößt, wird SD den Auftraggeber unverzüglich benachrichtigen (E-Mail zulässig).

4.2 SD kann auch Personenbezogene Daten verarbeiten, sofern dies nach geltendem Recht erforderlich ist. In einem solchen Fall wird SD den Auftraggeber vor der Verarbeitung über diese rechtlichen Anforderungen informieren, es sei denn, die betreffende Vorschrift verbietet solche Informationen.

4.3 Zur Verarbeitung Personenbezogener Daten gewähren SD und allfällige Unterauftragsverarbeiter nur befugten Personen Zugang, die sich zur Vertraulichkeit verpflichtet haben. SD und Unterauftragsverarbeiter werden die Personen, die Zugang

zu Personenbezogenen Daten haben, regelmäßig in Bezug auf die anwendbaren Datensicherheits- und Datenschutzmaßnahmen schulen.

4.4 Auf Wunsch des Auftraggebers wird SD angemessen mit dem Auftraggeber zusammenarbeiten, um allfällige Anfragen von Betroffenen Personen oder Aufsichtsbehörden bezüglich der Verarbeitung Personenbezogener Daten durch SD zu bearbeiten. SD wird den Auftraggeber so bald wie zumutbar möglich über jede Anfrage informieren, die SD von einer Betroffenen Person im Zusammenhang mit der Verarbeitung Personenbezogener Daten erhalten hat, ohne selbst auf diese Anfrage ohne weitere Weisungen des Auftraggebers zu antworten. SD stellt Funktionen zur Verfügung, die die Fähigkeit des Auftraggebers unterstützen, Personenbezogene Daten aus dem Cloud Service zu berichtigen oder zu löschen oder die Verarbeitung gemäß dem Datenschutzgesetz einzuschränken. Wenn eine solche Funktionalität nicht zur Verfügung gestellt wird, wird SD gemäß den Weisungen des Auftraggebers und dem Datenschutzrecht Personenbezogene Daten berichtigen oder löschen oder deren Verarbeitung einschränken.

4.5 SD wird dem Auftraggeber eine Verletzung des Schutzes Personenbezogener Daten unverzüglich nach Kenntniserlangung melden und ihm angemessene und SD vorliegende Informationen zur Verfügung stellen, um ihn bei der Erfüllung seiner Verpflichtungen zur Meldung einer Verletzung des Schutzes Personenbezogener Daten gemäß den Anforderungen des Datenschutzrechts zu unterstützen. SD kann diese Informationen in Abschnitten zur Verfügung stellen, je nachdem, zu welchem Zeitpunkt sie verfügbar werden. Eine solche Meldung ist kein Eingeständnis des Verschuldens oder der Haftung von SD und keinesfalls dahingehend auszulegen.

4.6 Wenn der Auftraggeber (oder seine für die Verarbeitung Verantwortlichen) gemäß Datenschutzrecht verpflichtet sind, eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation mit einer Aufsichtsbehörde durchzuführen, stellt SD auf Wunsch des Auftraggebers diejenigen Dokumente zur Verfügung, die für den Cloud Service allgemein verfügbar sind (z.B. diese AVV, die Vereinbarung oder allfällige Auditberichte oder Zertifizierungen). Jede zusätzliche Unterstützung wird zwischen den Vertragsparteien einvernehmlich vereinbart.

5 DATENSICHERHEIT

5.1 SD erklärt rechtsverbindlich, dass alle unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, des Kontextes und der Zwecke der Verarbeitung Personenbezogener Daten angemessen und erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen wurden. SD hat zu diesem Zweck die in Anhang 1 aufgeführten technischen und organisatorischen Maßnahmen umgesetzt und wird diese anwenden.

5.2 Änderungen. SD wendet die in Anhang 1 beschriebenen technischen und organisatorischen Maßnahmen auf alle SD-Kunden gleichermaßen an (ausgenommen die in Abschnitt 9 gelisteten Optionen), die im selben Rechenzentrum gehostet werden und den gleichen Cloud Service erhalten. SD kann die in Anhang 1 aufgeführten Maßnahmen jederzeit ohne Vorankündigung ändern, solange sie ein vergleichbares oder besseres Sicherheitsniveau aufrechterhält. Einzelne Maßnahmen können durch neue Maßnahmen ersetzt werden, die dem gleichen Zweck dienen, ohne das Sicherheitslevel zum Schutz Personenbezogener Daten zu beeinträchtigen.

6 DATEN-EXPORT & DATEN-LÖSCHUNG

6.1 Export und Entnahme durch den Auftraggeber: Während der Laufzeit und gemäß den Regelungen der Vereinbarung kann der Auftraggeber jederzeit auf seine Personenbezogenen Daten zugreifen. Der Auftraggeber kann seine Personenbezogenen Daten entnehmen und in einem Standardformat exportieren. Abruf und Export können technischen Beschränkungen und Voraussetzungen unterliegen. In diesem Fall werden sich SD und Auftraggeber auf eine angemessene Methode zur Ermöglichung des Zugriffs des Auftraggebers auf die Personenbezogenen Daten verständigen.

6.2 Löschung. Vor Vertragsende kann der Auftraggeber die jeweils verfügbaren Self-Service-Export-Tools von SD verwenden, um einen abschließenden Export der Personenbezogenen Daten aus dem Cloud Service durchzuführen (was einer Rückgabe der Personenbezogenen Daten entspricht). Der Auftraggeber erteilt SD hiermit die Weisung, nach Vertragsende die auf den zum Hosting des Cloud Service eingesetzten Servern verbliebenen Personenbezogenen Daten innerhalb einer angemessenen Zeit gemäß dem Datenschutzrecht zu löschen (spätestens innerhalb von 6 Monaten), es sei denn, deren Aufbewahrung ist nach anwendbarem Recht erforderlich.

7 UNTERAUFTRAGSVERARBEITER

7.1 SD erhält hiermit die schriftliche Genehmigung, die Verarbeitung von Personenbezogenen Daten unter den nachfolgenden Voraussetzungen auf Unterauftragsverarbeiter zu übertragen:

7.1.1. SD informiert den Auftraggeber vor Vertragsabschluss über Identität und Rolle des Unterauftragsverarbeiters, sofern der Einsatz nicht nur aufgrund der konkreten Anforderungen und Vorgaben des Auftraggebers notwendig wird;

7.1.2. SD beauftragt Unterauftragsverarbeiter im Rahmen schriftlicher Verträge (einschließlich elektronischer Form), die mit den Bestimmungen dieser AVV in Bezug auf die Verarbeitung Personenbezogener Daten durch den Unterauftragnehmer übereinstimmen. SD haftet für etwaige Verstöße durch den Unterauftragsverarbeiter gemäß den Bestimmungen dieser Vereinbarung;

7.1.3. SD wird die Sicherheits-, Datenschutz- und Vertraulichkeitspraktiken eines Unterauftragsverarbeiters vor dessen Auswahl bewerten, um festzustellen, dass er in der Lage ist, das in dieser AVV geforderte Schutzniveau für Personenbezogene Daten zu bieten.

7.2 Der Einsatz von neu hinzutretenden Unterauftragsverarbeitern erfolgt unter der Voraussetzung, dass folgende Regelungen eingehalten werden:

7.2.1. SD informiert den Auftraggeber im Voraus (per Email oder durch eine Information innerhalb des Cloud Service) über jegliche geplante Hinzufügungen oder Ersetzungen innerhalb der Liste der genehmigten Unterauftragsverarbeiter, einschließlich des Namens, der Anschrift und der Rolle des neuen Unterauftragsverarbeiters; und

7.2.2. der Auftraggeber kann solchen Änderungen gemäß dem nachfolgenden Abschnitt widersprechen.

7.3 Widerspruch gegen neue Unterauftragsverarbeiter.

7.3.1. Sofern der Auftraggeber gemäß Datenschutzrecht einen berechtigten Grund hat, der Verarbeitung Personenbezogener Daten durch die neuen Unterauftragsverarbeiter zu widersprechen und SD den Unterauftragsverarbeiter trotz Widerspruch des Auftraggebers einsetzt, kann er die Vereinbarung (beschränkt auf den Service-Teil, für den der neue Unterauftragsverarbeiter eingesetzt werden soll) durch schriftliche Erklärung gegenüber SD mit Wirkung zu einem vom Auftraggeber festgelegten Zeitpunkt kündigen, spätestens jedoch zum Ablauf von dreißig Tagen nach dem Datum der Mitteilung von SD an den Auftraggeber über den neuen Unterauftragsverarbeiter. Kündigt der Auftraggeber nicht innerhalb dieser Frist von dreißig Tagen, so gilt der neue Unterauftragsverarbeiter als durch den Auftraggeber genehmigt.

7.3.2. Innerhalb der Dreißig-Tagesperiode ab dem Datum der Mitteilung von SD an den Auftraggeber, in der der Auftraggeber über den neuen Unterauftragsverarbeiter informiert wird, kann der Auftraggeber verlangen, dass die Parteien in gutem Glauben zusammenkommen und eine Lösung des Widerspruchs besprechen. Diese Besprechungen verlängern die Kündigungsfrist nicht und berühren nicht das Recht von SD, den/die neuen Unterauftragsverarbeiter nach Ablauf der Frist von dreißig Tagen in Dienst nehmen zu dürfen.

7.3.3. Jede Kündigung nach diesem Abschnitt 7.3 wird von beiden Parteien als unverschuldet betrachtet und unterliegt den Bestimmungen der Vereinbarung.

7.4 Notfallaustausch: SD kann einen Unterauftragsverarbeiter ohne vorherige Mitteilung austauschen oder einsetzen, wenn sich der Grund für den Einsatz/Austausch der zumutbaren Kontrolle von SD entzieht und der umgehende Austausch aus Sicherheits- oder anderen dringenden Gründen erforderlich ist. In diesem Fall informiert SD den Auftraggeber über den neuen Unterauftragsverarbeiter unverzüglich nach seiner Ernennung. Abschnitt 7.3 gilt entsprechend.

8 INTERNATIONALE VERARBEITUNG

8.1 SD ist berechtigt, die Verarbeitung von Personenbezogene Daten unter Einbeziehung von Unterauftragsverarbeitern im Sinne dieser AVV außerhalb des Landes, in dem sich der Auftraggeber befindet, unter Einhaltung des Datenschutzrechts durchzuführen.

8.2 Grundsätzlich setzt SD nur innerhalb der Europäischen Union ansässige Unterauftragsverarbeiter ein.

8.3 Ohne ausdrückliche Zustimmung des Auftraggebers wird SD keine personenbezogenen Daten des Auftraggebers an in den USA ansässige Unterauftragsverarbeiter übermitteln, da nach derzeitigem Stand davon auszugehen ist, dass auch durch Verwendung von Standardvertragsklauseln die Gewährleistung eines angemessenen Datenschutzniveaus in den USA nicht möglich ist.

8.4 Sofern (i) Personenbezogene Daten eines im EWR oder der Schweiz ansässigen Verantwortlichen in einem Land außerhalb des EWR, der Schweiz bzw. außerhalb eines Landes, einer Organisation oder eines Gebiets verarbeitet werden, das von der Europäischen Union als sicheres Land mit einem angemessenen Datenschutzniveau gemäß Art. 45 DSGVO anerkannt ist, verarbeitet werden, oder (ii) Personenbezogene Daten eines anderen Verantwortlichen international verarbeitet werden und eine solche internationale Verarbeitung ein angemessenes Mittel nach dem anwendbaren Recht des Verantwortlichen erfordert, und das angemessene Mittel durch den Abschluss von Standardvertragsklauseln erfüllt werden kann, stellt SD sicher, dass Grundlage jeder solchen Verarbeitung die EU-Standardvertragsklauseln sind. Andernfalls erfolgt keine internationale Verarbeitung.

ANHANG 1

Technische und organisatorische Maßnahmen

In den folgenden Abschnitten werden die aktuellen technischen und organisatorischen Maßnahmen der SD definiert. SD kann diese Maßnahmen jederzeit unangekündigt ändern, solange eine vergleichbare oder höhere Sicherheitsstufe aufrechterhalten oder erreicht wird. Einzelne Maßnahmen können durch neue Maßnahmen, die denselben Zweck erfüllen, ersetzt werden, ohne dass die Sicherheitsstufe beim Schutz Personenbezogener Daten verringert wird.

1 Zutrittskontrolle

1.1 Unbefugten wird der physische Zugang zu Einrichtungen, Gebäuden und Räumlichkeiten verwehrt, in denen sich Datenverarbeitungssysteme befinden, die Personenbezogene Daten verarbeiten oder nutzen.

1.2 Maßnahmen:

- SD schützt Gebäude durch angemessene Maßnahmen basierend auf der SD Security Policy.
- Im Allgemeinen sind Gebäude durch Zutrittskontrollsysteme (z.B. Zutritt per Chipkarte) gesichert.
- Als Mindestanforderung müssen die äußeren Zugänge eines Gebäudes mit einer zertifizierten Schließanlage ausgestattet sein, einschließlich einer modernen, aktiven Schlüsselverwaltung.
- Abhängig von der Sicherheitseinstufung werden Gebäude, einzelne Bereiche und das umliegende Gelände möglicherweise durch weitere Maßnahmen geschützt. Dazu gehören spezielle Zutrittsprofile, Videoüberwachung, Einbruchmeldeanlagen und biometrische Zutrittskontrollsysteme.
- Die Vergabe der Zutrittsrechte an die berechtigten Personen erfolgt auf individueller Basis gemäß den Maßnahmen zur System- und Datenzugriffskontrolle (siehe folgende Abschnitte 1.2 und 1.3). Dies gilt auch für den Zutritt von Besuchern. Gäste und Besucher in SD-Gebäuden müssen sich namentlich an der Rezeption anmelden und von autorisiertem SD-Personal begleitet werden.
- Zusätzliche Maßnahmen für Rechenzentren:
    - Biometrisches Zutrittskontrollsystem (mittels Fingerabdruck)
    - Kontaktlose Schlüsselkarte
    - Vereinzelungsanlage
    - Einzeln versperrte Serverschränke (dokumentierte Schlüsselvergabe)
    - Sicherheitszonen und räumliche Trennung (Rechenzentrum > Raum > Cage im Raum > Serverschrank)
    - 24/7 Videoüberwachung
    - 24/7 Sicherheitspersonal im Rechenzentrum
    - ISO27001 Zertifizierung
    - ISO9001 Zertifizierung

2 Systemzugriffskontrolle

2.1 Datenverarbeitungssysteme, die zur Bereitstellung des Cloud Service genutzt werden, sind vor einer nicht autorisierten Nutzung zu schützen.

2.2 Maßnahmen:

- Die Gewährung des Zugriffs auf sensible Systeme, einschließlich der Systeme zur Speicherung und Verarbeitung Personenbezogener Daten, erfolgt über mehrere Berechtigungsstufen.
- Berechtigungen werden über definierte Prozesse gemäß der SD Security Policy verwaltet.
- Alle Personen greifen mit einer eindeutigen Kennung (User-ID) auf die Systeme von SD zu
- SD hat Verfahren eingerichtet, so dass angeforderte Änderungen an Berechtigungen nur in Übereinstimmung mit der SD Security Policy durchgeführt werden (beispielsweise werden keine Rechte ohne entsprechende Berechtigung erteilt). Wenn ein Mitarbeiter das Unternehmen verlässt, werden dessen Zugriffsrechte aufgehoben.
- SD hat eine Kennwortrichtlinie festgelegt, die die Weitergabe von Kennwörtern untersagt, regelt, wie vorzugehen ist, wenn ein Kennwort offengelegt wird, und erfordert, dass Kennwörter regelmäßig geändert und vorgegebene Kennwörter geändert werden. Zur Authentifizierung werden personalisierte Benutzerkennungen (User-IDs) zugewiesen. Alle Kennwörter müssen bestimmte Mindestbedingungen erfüllen und werden in verschlüsselter Form gespeichert. Im Fall von Domänenkennwörtern erzwingt das System alle sechs Monate eine Änderung des Kennworts, das den Anforderungen an komplexe Kennwörter entsprechen muss. Jeder Computer verfügt über einen kennwortgeschützten Bildschirmschoner.

- Das Unternehmensnetzwerk ist durch Firewalls vor dem öffentlichen Netzwerk geschützt.
- SD verwendet aktuelle Virenscanner an den Übergängen zum Firmennetz (für E-Mail-Konten), sowie auf allen Fileservern und auf allen Einzelplatzcomputern.
- Das Sicherheitspatch-Management gewährleistet die Anwendung entsprechender regelmäßiger Sicherheits-Updates. Der vollständige Zugriff auf das SD-Firmennetzwerk und die kritische Infrastruktur ist durch eine strenge Authentifizierung geschützt.

3 Datenzugriffskontrolle

3.1 Personen, die zur Nutzung von Datenverarbeitungssystemen berechtigt sind, erhalten nur Zugriff auf die Personenbezogenen Daten, für die sie Zugriffsrechte besitzen, und Personenbezogene Daten dürfen bei der Verarbeitung, Nutzung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

3.2 Maßnahmen:

- Im Rahmen der SD Security Policy erfordern Personenbezogene Daten zumindest den Gleichen Schutz wie „vertrauliche“ Informationen im Sinne des SD-Informationsklassifizierungsstandards.
- Der Zugriff auf Personenbezogene Daten wird nur bei entsprechender Notwendigkeit gewährt („Need-to-know“-Prinzip). Jeder Person wird der Zugriff nur auf diejenigen Informationen gewährt, die sie zur Erledigung ihrer Pflichten benötigt. SD verwendet Berechtigungskonzepte, die die Zuweisungsprozesse und die zugewiesenen Rollen pro Account (User ID) dokumentieren. Alle Auftraggeberdaten werden gemäß der SD Security Policy geschützt.
- Alle produktiven Server werden in Rechenzentren oder in sicheren Serverräumen betrieben. Die Sicherheitsmaßnahmen zum Schutz der Anwendungen zur Verarbeitung Personenbezogener Daten werden in regelmäßigen Abständen geprüft. Zu diesem Zweck führt SD interne und externe Sicherheitsüberprüfungen und Penetrationstests ihrer IT-Systeme durch.
- SD erlaubt nicht die Installation eigener Software oder sonstiger Software, die nicht durch SD genehmigt wurde.
- Durch einen entsprechenden SD-Sicherheitsstandard wird geregelt, auf welche Weise Daten und Datenträger gelöscht oder vernichtet werden, wenn sie nicht mehr benötigt werden.

4 Datenübertragungskontrolle

4.1 Die Datenübertragungskontrolle gewährleistet, dass Personenbezogene Daten, außer soweit für die Erbringung der Cloud Services gemäß der Vereinbarung notwendig, bei der Übertragung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Beim physischen Transport von Datenträgern werden bei SD geeignete Maßnahmen getroffen, um die vereinbarten Service-Level zu gewährleisten (z. B. Verschlüsselung, mit Blei ausgekleidete Behälter).

4.2 Maßnahmen:

- Personenbezogene Daten sind bei der Übertragung über interne SD-Netzwerke geschützt gemäß der SD Security Policy geschützt.
- Im Hinblick auf die Übertragung der Daten zwischen SD und ihren Auftraggebern werden die Sicherheitsmaßnahmen für die übertragenen Personenbezogenen Daten von den Parteien vereinbart und zum Bestandteil der Vereinbarung. Dies gilt sowohl für die physische als auch für die netzwerkbasierte Datenübertragung. In jedem Fall übernimmt der Auftraggeber die Verantwortung für die Datenübertragung, sobald sie außerhalb der von SD kontrollierten Systeme erfolgt (z. B. Daten, die außerhalb der Firewall des SD-Rechenzentrums übertragen werden).

5 Dateneingabekontrolle

5.1 Es wird die Möglichkeit geschaffen, im Nachhinein zu untersuchen und festzustellen, ob und von wem Personenbezogene Daten erfasst, modifiziert oder aus den Datenverarbeitungssystemen der SD entfernt wurden.

5.2 Maßnahmen:

- SD gestattet ausschließlich befugten Personen im Rahmen ihrer Pflichten, auf Personenbezogene Daten zuzugreifen.
- SD hat innerhalb des Cloud Service ein Protokollierungssystem für das Erfassen, Ändern und Löschen oder Sperren Personenbezogener Daten durch SD oder ihre Unterauftragsverarbeiter im technisch möglichen Umfang implementiert.

6 Auftragskontrolle

6.1 Personenbezogene Daten, die im Auftrag verarbeitet werden (z. B. im Auftrag des Auftraggebers), werden ausschließlich in Übereinstimmung mit der Vereinbarung und den diesbezüglichen Weisungen des Auftraggebers verarbeitet.

6.2 Maßnahmen:

- SD nutzt Kontrollen und Verfahren, um die Einhaltung der Verträge zwischen SD und ihren Auftraggebern, Unterauftragsverarbeitern oder anderen Serviceanbietern zu überwachen.
- Im Rahmen der SD Security Policy erfordern Personenbezogene Daten zumindest den Gleichen Schutz wie „vertrauliche“ Informationen im Sinne des SD-Informationsklassifizierungsstandards.

- Sämtliche SD-Mitarbeiter und Unterauftragsverarbeiter oder anderen Serviceanbieter werden vertraglich verpflichtet, die Geheimhaltungspflicht in Bezug auf alle sensiblen Informationen einschließlich Geschäftsgeheimnissen von Auftraggebern und Partnern der SD einzuhalten.

7 Verfügbarkeitskontrolle

7.1 Personenbezogene Daten werden vor versehentlicher oder nicht autorisierter Vernichtung oder Verlust geschützt.

7.2 Maßnahmen:

- SD verfügt über regelmäßige Backup-Prozesse zur Wiederherstellung der Verfügbarkeit geschäftskritischer Systeme bei Bedarf.
- SD verwendet unterbrechungsfreie Stromversorgungen (USV, Batterien, Generatoren usw.), um die Stromversorgung für die Rechenzentren zu schützen.
- SD hat Geschäftseventualfallpläne für geschäftskritische Prozesse ausgearbeitet und kann Desaster Recovery Strategien für geschäftskritische Services anbieten, wie näher in der Dokumention beschrieben oder in der Bestellung für den jeweiligen Cloud Service einbezogen.
- Notfallprozesse und -systeme werden regelmäßig getestet.

8 Trennungskontrolle

8.1 Personenbezogene Daten, die für unterschiedliche Zwecke erfasst werden, können getrennt verarbeitet werden.

8.2 Maßnahmen:

- SD nutzt die technischen Möglichkeiten der implementierten Software (z. B. Multi-Tenancy- oder getrennte Systemlandschaften), um die Trennung von Personenbezogenen Daten zu ermöglichen, die von verschiedenen Auftraggebern stammen.
- Der Auftraggeber (einschließlich seiner Verantwortlichen) hat ausschließlich auf seine eigenen Daten Zugriff.
- Wenn zur Bearbeitung eines Supportfalls des Auftraggebers Personenbezogene Daten dieses Auftraggebers benötigt werden, werden die Daten dieser Meldung zugeordnet und nur zur Bearbeitung dieser Meldung verwendet; für die Bearbeitung anderer Meldungen findet kein Zugriff auf diese Daten statt. Diese Daten werden in dedizierten Support-Systemen gespeichert.

9 Datenintegritätskontrolle

9.1 Personenbezogene Daten bleiben während der Verarbeitungsaktivitäten unversehrt, vollständig und aktuell.

9.2 Maßnahmen:

SD hat zum Schutz vor unautorisierten Änderungen eine mehrere Schichten umfassende Sicherheitsstrategie umgesetzt. Insbesondere verwendet SD die folgenden Mittel, um die obigen Abschnitte zu Kontrollen und Maßnahmen umzusetzen:

- Firewalls
- Security Monitoring
- Antivirensoftware
- Erstellen von Sicherungskopien und Wiederherstellung
- Externe und interne Penetrationstests
- Regelmäßige Prüfung der Sicherheitsmaßnahmen durch externe Prüfer