1 Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)

1.1 Pseudonymisierung

Maßnahmen zur Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen

1.1.1 **RZ-Outsourcing / (Virtual) Private Cloud / Dienstleistungen ohne direkte RZ-Anbindung**

Personenbezogene Daten werden, soweit möglich und vom Auftraggeber angewiesen, für Verarbeitungen pseudonymisiert:
Durch die Anwendung der Pseudonymisierung auf personenbezogene Daten kann ein Risiko für die betreffende Person gesenkt werden.

Es besteht eine Festlegung der Rollen, welche zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind.

Eine Pseudonymisierung kann durch eine Verschlüsselung oder durch das Entfernen sämtlicher personenbezogener Daten für bestimmte Verarbeitungen erfolgen. Hierfür sind die personenbezogenen und personenbeziehbaren Daten für den Empfänger nicht mehr erkennbar und nur noch durch eine identische Kennziffer mit den restlichen Daten zu verbinden, z.B. Trennung von Kundenstammdaten und Kundenumsatzdaten. Die Verarbeitung erfolgt über eine Kennziffer statt über den Namen. Die Vorgaben werden zwischen dem Auftraggeber und dem Auftragnehmer vor der Umsetzung abgestimmt und in den Leistungsscheinen konkretisiert.

1.1.2 **Public Cloud**

Personenbezogene Daten werden, soweit möglich und vom Auftraggeber angewiesen, für Verarbeitungen pseudonymisiert. Es besteht eine Festlegung der Rollen, welche zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind.

1.2 Verschlüsselung

Einsatz von Verfahren und Algorithmen, die personenbezogene Daten mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht lesbare Form umwandeln. Es kommen symmetrische und asymmetrische Verschlüsselungstechniken in Betracht

1.2.1 **RZ-Outsourcing / (Virtual) Private Cloud / Dienstleistungen ohne direkte RZ-Anbindung**

Im Sinne der Auftragsverarbeitung entscheidet allein der Auftraggeber, wann welche Verschlüsselung eingesetzt werden kann, dieses können z.B. sein: Data at Transport – Data at Rest – Ende-zu-Ende.

Ein Fernzugriff (Remote) erfolgt über eine VPN (Virtual Private Network) Anbindung oder verschlüsselt zum Terminal Server.

Mobile Datenträger, welche personenbezogene Daten oder Betriebs- und Geschäftsunterlagen enthalten müssen immer verschlüsselt werden.

Unterschiedliche Optionen zur symmetrischen oder asymmetrischen Verschlüsselung können auf Anfrage des Verantwortlichen zum Schutz seiner personenbezogenen Daten umgesetzt und in den Leistungsscheinen konkretisiert werden (z.B. Nutzung von SSL-Zertifikaten für eine verschlüsselte Web-Kommunikation, SSL-Virtual Private Netzwerk für eine gesicherte Verbindung).

Die Verschlüsselungen entsprechen dem Stand der Technik.

1.2.2 **Public Cloud**

Im Sinne der Auftragsverarbeitung entscheidet allein der Auftraggeber, wann welche Verschlüsselung eingesetzt werden kann. Die Schlüssel sind vor dem nicht autorisierten Zugriff zu schützen.

Ein Zugriff oder die Nutzung von Inhalten erfolgt nicht, es sei denn, es ist notwendig, um die Serviceangebote zu warten oder anzubieten, oder erforderlich, um die Gesetze einzuhalten oder einer verbindlichen Anordnung einer staatlichen Stelle nachzukommen.

2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren

2.1.1 **RZ-Outsourcing / (Virtual) Private Cloud**

Die Räume der Data Center schützen die Infrastruktur der Auftraggeber vor unberechtigtem Zutritt und sichern zudem die Hochverfügbarkeit der Gebäudetechnik für den Rechenzentrumsbetrieb ab.

Die Gelände, auf denen sich die Rechenzentren befinden, unterliegen strengen Sicherheitsvorgaben zur Zutrittsberechtigung.

Der Zutritt zu den Rechenzentren ist durch verschiedene, unabhängige Zutrittssysteme nur autorisierten Personen gestattet.

Alle Besucher der Rechenzentren werden mit Datum und Uhrzeit ihres Betretens und Verlassens von den Mitarbeitern erfasst. Der Zutritt zum Gelände wird zudem nur für spezielle autorisierte Zwecke eingeräumt und soweit notwendig, werden Instruktionen im Hinblick auf die Sicherheitsanforderungen des Bereichs und zu Notfallverfahren erteilt. Die Autorisierung für den Zutritt zum Rechenzentrum setzt eine Unterschrift unter die persönliche Einwilligung zur Befolgung der Verhaltensregeln und Richtlinien innerhalb der Rechenzentrumsbereiche voraus.

An einigen Standorten patrouilliert der Werkschutz in unregelmäßigen Abständen über das Gelände, zusätzlich sind alle Gebäudeteile des Rechenzentrums mit Einbruchmeldeanlagen geschützt. Ebenfalls erfassen Kameraüberwachungen die Innen- und Außenzugänge der Rechenzentren rund um die Uhr.

Innerhalb der Gebäude können an unterschiedlichen Standorten verschiedene Sicherheitszonen definiert sein, hier sind zu benennen z. B. Leitstandzone, Serverflächen, Datenarchiv, Segmente des Auftraggebers. Der Zutritt erfolgt generell über eine persönlich zugeordnete und kontrollierbare Zutrittskarte der berechtigten Personen. Die Berechtigung für die einzelnen Zonen wird über einen Autorisierungsprozess gesichert und erfolgt ausschließlich gemäß der Notwendigkeit für das Geschäftsmodell.

Jeder externe Besucher wird von einem internen Mitarbeiter während des gesamten Besuches im RZ begleitet. Dienstleistern ist der Aufenthalt in den Räumen des RZ nur unter Aufsicht gestattet.

2.1.2 **Dienstleistungen ohne direkte RZ-Anbindung**

Für sämtliche Standorte oder Verarbeitungen ohne direkten RZ-Bezug gelten folgende physische Sicherheitsmaßnahmen.

Zutrittskontrollen gewährleisten einen ausschließlich autorisierten Zutritt für Mitarbeiter des Unternehmens. Der autorisierte Zutritt in Büros erfolgt je nach Standort in der Regelarbeitszeit durch Vereinzelungsschleusen, eine zweite Sicherheitstür, Schließanlagen, Schließzylinder, Türtransponder, autorisierte Mitarbeiterausweise (RFID-Ausweis), automatisierte Zutrittskontrollsysteme (Kartenleser) mit personalisierten Zutrittskarten, Zugangskeys für autorisierte internen Mitarbeiter. Die Schlüsselausgabe wird in einem Schlüsselbuch dokumentiert.

Besucher werden am Eingang durch einen Ansprechpartner abgeholt und während des gesamten Aufenthaltes in den Räumlichkeiten begleitet.

Teilweise patrouilliert der Werkschutz in unregelmäßigen Abständen das Gelände oder die Gebäudeteile sind mit Einbruchmeldeanlagen geschützt. Ebenfalls erfasst an einigen Standorten eine Kameraüberwachung für Innen- und Außenanlagen rund um die Uhr den Eingangsbereich, die Lobby, die Liftanlagen als auch die Zugänge zu den Bürobereichen.

2.1.3 **Public Cloud**

Die Gebäude werden bei einigen Cloudanbietern von Wachschutzpersonal betreut und überwacht und bei sensiblen Bereichen zusätzlich mit Video überwacht.

Es existiert ein Zutrittsberechtigungskonzept, dem sowohl ein Schließsystem, zum Teil mit einer ordnungsgemäßen Schlüsselverwaltung, als auch ein elektronisches Zutrittskontrollsystem zu Grunde liegt.

Der Zugang zu einzelnen Produktionsbereichen und dem Geschäftsbereich wird über ein elektronisches Zutrittskontrollsystem unter Einsatz z.B. von Magnetkarten beschränkt.

Besuchern ist der Zugang zu sensiblen Bereichen nur nach vorheriger Anmeldung gestattet. Im Zuge der Akkreditierung erhält der Besucher eine Kennzeichnung, z.B. einen Besucherausweis, welche ihn als Gast ausweist und die er während des Aufenthaltes am Standort bei sich tragen muss. An einigen Standorten ist über eine Richtlinie der Umgang mit Gästen definiert. Der Zugang zu den einzelnen Produktionsbereichen ist nur in Begleitung von autorisiertem Personal gestattet.

2.2 Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

2.2.1 **RZ-Outsourcing / (Virtual) Private Cloud**

Alle Systeme und Anwendungen erfordern eine Authentifizierung zur Nutzung der Dienste.

Der Zugriff auf die verarbeitenden Systeme erfolgt mit einer eindeutigen persönlichen User-ID und einem Passwort. Die Passwortvergabe erfolgt in Konformität zur Passwortrichtlinie. Hier sind z.B. zu benennen: Anforderungen an die Passwortgüte, erzwungene Passwortänderungen oder nach Mehrfachanmelden mit falschem Passwort eine Sperrung des Benutzerkontos zur Vermeidung des Risikos (um Brute-Force-Attacken zu verhindern).

Für die Mitarbeiter wird ein Starter-Changer-Leaver Prozess durchlaufen. Hier wird durch die verantwortlichen Führungskräfte zur Durchführung einer Benutzerkontrolle die Autorisierung basierend auf dem „least privilege principle“ vorgenommen.

Systemadministration und reguläre Benutzer erhalten getrennte Benutzerkonten. Ebenfalls findet für privilegierte Rechte ein regelmäßiger Check bzgl. vorhandener Autorisierung statt.

Zur Vermeidung des Risikos ist bei Remote Zugriff auf das Netzwerk die Nutzung von 2-Faktor-Authentifizierungsmethoden (Secure-ID Karten oder Zertifikate) in der Informationssicherheitsrichtlinie vorgeschrieben.

Der Schutz sämtlicher Netzwerke gegen Zugriffe von außen wird durch Firewalls reguliert und erfolgt standartmäßig über eine Sicherheitsinfrastruktur-Kette aus Proxy, Virenscanner und Firewall. An einigen Standorten kann hierfür die spezielle Rolle des Network Security Officer zuständig sein.

Es ist möglich ein Intrusion Prevention System (IPS) zur aktiven Bekämpfung von Netzwerkangriffen (Remote Access, Access Control-Listen, spezielle WAN Bereiche, etc.) zur Verfügung zu stellen, welches nach Beauftragung im Leistungsschein für die unterschiedlichen Verarbeitungen definiert und eingepreist wird.

2.2.2 **Dienstleistungen ohne direkte RZ-Anbindung**

Für die Mitarbeiter wird ein Starter-Changer-Leaver Prozess durchlaufen. Hier wird durch die verantwortlichen Führungskräfte die Autorisierung basierend auf dem „least privilege principle“ vorgenommen.

Der Zugriff auf die verarbeitenden Systeme erfolgt mit einer eindeutigen persönlichen User-ID und einem Passwort. Die Passwortvergabe erfolgt in Konformität zur Passwortrichtlinie. Hier sind z.B. zu benennen: Anforderungen an die Passwortgüte, erzwungene Passwortänderungen oder nach Mehrfachanmelden mit falschem Passwort eine Sperrung des Benutzerkontos zur Vermeidung des Risikos (um Brute-Force-Attacken zu verhindern).

Für privilegierte Rechte findet ein regelmäßiger Check der vorhandenen Autorisierungen statt. Systemadministratoren und reguläre Benutzer erhalten getrennte Benutzerkonten.

Zur Vermeidung des Risikos ist bei Remote Zugriff auf das Netzwerk die Nutzung von 2-Faktor-Authentifizierungsmethoden (Secure-ID Karten oder Zertifikate) in der Informationssicherheitsrichtlinie vorgeschrieben.

Der Schutz sämtlicher Netzwerke gegen Zugriffe von außen wird durch Firewalls reguliert und erfolgt standartmäßig über eine Sicherheitsinfrastruktur-Kette aus Proxy, Virenscanner und Firewall. An einigen Standorten kann hierfür die spezielle Rolle des Network Security Officer zuständig sein.

2.2.3 **Public Cloud**

Es bestehen Regelungen für den Zugriff auf EDV Systeme.

Diese Regelungen (z.B. die Kennwortkonvention) fordert u.a. eine Mindestlänge und Anforderungen für Passwörter (z.B. Groß- und Kleinschreibung, Zahlen und Sonderzeichen, maximale Gültigkeitsdauer, Trivialkennwortprüfung).

Die An- und Abmeldungen der Benutzer an den DV-Anlagen werden protokolliert.

Beim Verlassen des Arbeitsplatzes ist dieser zu sperren oder herunterzufahren. Wird dies vergessen, sperrt sich der Arbeitsplatz automatisch.

Zudem existiert ein Zugangsberechtigungskonzept. Generell sind alle Berechtigungen entzogen und müssen freigeschaltet werden. Das Zugangsberechtigungskonzept basiert auf dem Prinzip von Benutzerrollen und -profilen. Die Vergabe der personalisierten Berechtigungen erfolgt durch die zuständige Abteilung.

Auf Anfrage können Auszüge und Zusammenfassungen aus entsprechenden Regelungen zur Verfügung gestellt werden.

2.3 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

2.3.1 **RZ-Outsourcing / (Virtual) Private Cloud / Dienstleistungen ohne direkte RZ-Anbindung**

Die Zugriffskontrolle basiert auf einem rollenbasierten Berechtigungskonzept für Systemzugriffe und abgestufte Administrationsrechte, entsprechend der Aufgabengebiete. Alle administrativen Tätigkeiten werden grundsätzlich auf den Systemen protokolliert und können somit nachvollzogen werden. Die Zugriffrechte werden nach dem Minimalprinzip / “Need-To-Know“-Prinzip vergeben. Es werden nur so viele Zugriffsrechte vergeben, wie es für die Aufgabenwahrnehmung notwendig ist. Die Einhaltung des „Need-To-Know“-Prinzips liegt in der Verantwortung der autorisierten Führungskraft.

Bei der Einrichtung eines Zuganges erhält der Benutzer nur minimale Standardberechtigungen. Diese dürfen nur über festgelegte Beantragungswege erweitert werden, wobei die jeweiligen Vorgesetzten bzw. Verantwortlichen zur Einhaltung einer angemessenen Funktionstrennung im Berechtigungsprozess ihre Zustimmung geben müssen (4-Augen-Prinzip).

Ein Fernzugriff (Remote) erfolgt über eine VPN (Virtual Private Network) Anbindung oder verschlüsselt zum Terminal Server.

2.3.2 **Public Cloud**

Es besteht ein Berechtigungskonzept für den Zugriff auf die DV-Systeme.

Ziel ist es, eine sichere, übersichtliche und einheitliche Freigabe– und Berechtigungsstrategie auf allen DV-Systemen bereitzustellen. Zugriffe erfolgen nach dem „Least-Privilege“-Konzept.

Es sind nur autorisierte Speichermedien zu verwenden. Mitarbeiter des Cloudanbieters unterliegen weitergehenden Restriktionen und Zustimmungserfordernissen, um personenbezogene Daten des Auftraggebers auf mobilen Datenträgern zu speichern oder außerhalb der Betriebsstätten des Cloudanbieters zu verarbeiten bzw. von dort auf dies zuzugreifen.

Der Zugriff auf die einzelnen Systeme wird über spezielle Netzwerkberechtigungen und ein mandantenbasiertes Rollenkonzept gesteuert (z.B. Administrator, IT etc.). Zugriffsrechte werden entsprechend dokumentiert. Zugriffsberechtigungen werden entzogen bzw. gelöscht.

Der Cloudanbieter informiert sein Personal über alle relevanten Prozesse und Rollenkonzepte und beschreibt Folgen der Verletzung entsprechender Vorgaben.

Auf Anfrage können Auszüge und Zusammenfassungen aus entsprechenden Konzepten zur Verfügung gestellt werden.

2.4 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes 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

2.4.1 **RZ-Outsourcing / (Virtual) Private Cloud / Dienstleistungen ohne direkte RZ-Anbindung**

Um das Risiko für den Betroffenen zu vermindern sind die Mitarbeiter angewiesen, nur sichere Datenübertragungswege zu nutzen, welche in der Datenschutzrichtlinie verpflichtend definiert sind. Die mögliche Datenübertragung kann über vertrauenswürdige Leitungen und Netze, welche ein Mitprotokollieren nicht ohne Weiteres ermöglichen, erfolgen.

Unterschiedliche Optionen, wie beispielsweise die Nutzung von SSL-Zertifikaten für eine verschlüsselte Web-Kommunikation, SSL-Virtual Private Netzwerk für eine gesicherte Verbindung (abgesicherter Remote Access), Elektronische Signatur, Protokollierung, können auf Anfrage umgesetzt und in den Leistungsscheinen dokumentiert und bewertet werden.

Im Sinne der Auftragsverarbeitung entscheidet allein der Auftraggeber, welche Daten übermittelt werden, welcher Übertragungsweg und welche Übertragungsart umgesetzt werden. Hier können Netzsegmente zusätzlich durch Access Control-Listen voneinander abgeschottet und das gesamte Netzwerk durch mehrstufige Firewall-Systeme abgesichert werden. Muss bei der Übertragung eine nicht vertrauenswürdige Datenleitung verwendet werden, so kann die Übertragung auch verschlüsselt (z.B. über Virtual Private Network - VPN, Transport Layer Security - TLS, etc.) erfolgen.

Für die Sicherung (Backup) von Daten werden bewegliche Datenträger und VTL-Libraries genutzt, welche einer automatischen Inventarisierung unterworfen sind und in einem Sicherheitsbereich lagern.

Zur Gewährleistung einer Transportkontrolle erfolgt ein Transport oder Versand von Datenträgern nur, wenn dieser vom Auftraggeber angewiesen wurde. Dieser bestimmt ebenfalls den Transportweg, welcher beispielsweise der Versand per Einschreiben/Wertpaket oder die Verwendung gesicherter/verschlossener Transportbehältnisse sowie spezieller Kurierdienste (verschlüsselter Versand) umfasst. Dieses unterliegt einem Kontroll- und Dokumentationsprozess.

Eine notwendige Vernichtung von Datenträgern erfolgt durch ein spezialisiertes und zertifiziertes Unternehmen nach aktuellen Normen. Bis zur Vernichtung lagern die Datenträger in einem Sicherheitsbereich und sind vor unbefugtem Zugriff geschützt. Die Vernichtung von Datenträgern des Verantwortlichen und die Protokollierung dieser Vernichtung erfolgt nur gemäß Beauftragung und Weisung.

Für die Nutzung von mobilen Datenträgern (USB-Stick, CD, DVD, etc.) existieren Verhaltensregeln in der Informationssicherheitsrichtlinie. Diese stellen sicher, dass personenbezogene Daten oder Betriebs- und Geschäftsunterlagen auf mobilen Datenträgern nur verschlüsselt abgelegt werden dürfen. Dieses verhindert im Rahmen der Datenträgerkontrolle das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern.

Für die sichere Vernichtung bzw. die Entsorgung von Datenträgern und vertraulicher Dokumente existieren Verhaltensregeln.

2.4.2 **Public Cloud**

Datenübertragungen erfolgen innerhalb des gesicherten Netzwerkes (z.B. mit entsprechender Verschlüsselung). Die elektronische Übertragung von Daten auf öffentlichen Wegen bzw. über öffentliche Netze findet ausschließlich auf verschlüsselten Wegen statt. Dabei finden in Abstimmung mit den Empfängern unterschiedliche Verfahren Anwendung.

Der Einsatz portabler Devices (z.B. deren Verbindung mit einem System) unterliegt besonderen Regelungen. Nicht mehr benötigte Geräte werden unter Beachtung des Schutzes personenbezogener Daten sachgerecht entsorgt (z.B. physische Vernichtung). Es kommen zudem verschiedene Schutzmechanismen zum Schutz der Datenbestände zum Einsatz (z.B. Firewalls, Regelungen zu konkreten Verfahren bei Zwischenfällen).

Auf Anfrage können Auszüge und Zusammenfassungen aus entsprechenden Konzepten zu entsprechenden Verfahren zur Verfügung gestellt werden.

2.5 Trennungskontrolle

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

2.5.1 **RZ-Outsourcing / (Virtual) Private Cloud / Dienstleistungen ohne direkte RZ-Anbindung**

Eine Trennung der Daten erfolgt auf Weisung des Auftraggebers für seine Daten. Die unterschiedlichen Optionen werden im Leistungsschein für die unterschiedlichen Verarbeitungen definiert und bewertet.

Als Beispiele für eine logische oder physische Trennung auf Mandanten- und/oder Datenebene können benannt werden: die Funktionstrennung Produktion / Integration / Test, Einsatz verschiedener Datenbanken, Einsatz von Zugriffskontrollsoft-

ware und Einrichtung von Zugriffsrechten (mit deren Protokollierung), unterschiedliche Verschlüsselung für einzelne Datensätze, logische Trennung (z.B. auf gesharten Systemen), physische Trennung (z.B. auf dedizierten Systemen), etc.

Bei einer Tätigkeit über Remote greift der Mitarbeiter auf die bereits vorgegebene Infrastruktur zu, welche ihm eine Verarbeitung im Rahmen der vorher festgelegten Vorgaben ermöglicht.

2.5.2 **Public Cloud**

In Anlehnung an das Berechtigungskonzept werden auf den Systemen Maßnahmen wie z.B. Verzeichnisse eingerichtet, die eine stringente Trennung von Daten und Dateien gegenüber weiteren Mandanten gewährleistet. Der Zugriff von Kunden auf Instanzen, die nicht den Zugriffsberechtigungen entsprechen, wird wirkungsvoll unterbunden.

Test-, Produktiv- sowie Integrationssysteme werden voneinander getrennt betrieben.

3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Eingabekontrolle

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

3.1.1 **RZ-Outsourcing / (Virtual) Private Cloud / Dienstleistungen ohne direkte RZ-Anbindung**

Eine Eingabekontrolle, sowie die Aufbewahrungsfrist der hierdurch entstandenen Daten, erfolgt auf Weisung durch den Auftraggeber für seine Daten und auf seiner Infrastruktur oder in seinen Applikationen.

Optionale Protokollierungen sowie revisionssichere Ablage der Logs sind auf Weisung umsetzbar und müssen im Rahmen des Leistungsscheines definiert werden.

Administrative Zugriffe auf Systeme können durch ein Standard-Logging auf Betriebssystemebene nachvollzogen werden. Dieses dient zum Nachweis einer unbefugten Veränderung oder Löschung von gespeicherten personenbezogenen Daten im Rahmen der Speicherkontrolle.

Eine Auswertung der Eingabekontrolle erfolgt nur bei Bedarf im Rahmen der Weisung durch eine manuelle oder automatisierte Protokollauswertung.

3.1.2 **Public Cloud**

Sofern die Eingabe, Veränderung sowie Löschung der Daten auf IT Systemen erfolgen, werden mittels entsprechender Protokollierungs- und Protokollauswertungssysteme die Veränderungen an diesen Daten protokolliert (z.B. Zugriffs-ID, Zugriffszeit, Autorisierung und entsprechende Aktivität).

Auf Anfrage können Auszüge und Zusammenfassungen aus entsprechenden Konzepten zu entsprechenden Verfahren zur Verfügung gestellt werden.

3.2 Organisatorische und technische Absicherung von Berechtigungen, Protokollierungsmaßnahmen, Protokoll-Auswertungen /Revision etc.

Weiterführende Ausführungen zur Absicherung von Berechtigungen sind im Kapitel Zugangs- und Zugriffskontrolle ausführlich dokumentiert. Protokollauswertungen sind im Rahmen der Weisung zu beantragen und werden in diesem Umfang durchgeführt. Eine Konkretisierung ist im jeweiligen Leistungsschein aufzunehmen.

4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Verfügbarkeitskontrolle

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

4.1.1 **RZ-Outsourcing / (Virtual) Private Cloud**

Sämtliche Einrichtungen des Rechenzentrums sind physisch gegen Sicherheitsbedrohungen und Umweltgefahren geschützt.

Unterschiedliche abgestufte Sicherheitseinrichtungen, zur Sicherstellung der Verfügbarkeit, können für das Geschäftsmodell im Leistungsschein definiert und konkretisiert werden.

Hier einige Möglichkeiten: redundante Stromzuführung, hochverfügbare Stromversorgung (teilweise abgesichert durch USV) mit statischen Übergabeschaltern (STS), Dieselaggregate für die Notstromversorgung, Klimatisierung mit hoher Verfügbarkeit, Brandmeldeanlagen mit Brandfrüherkennung und direkter Alarmmeldung bei der örtlichen Feuerwehr, je Rechenzentrum einen eigenen Brandabschnitt, Einbruchmeldeanlage mit Türschließkontrolle, Notfallkonzepte und Havarieplan, redundante Netzanbindungen und Netzwerkinfrastruktur, geclusterte Systeme oder redundante Hardware (von Bauelementen bis zu ganzen Servern – Geo-Redundanz).

Diese Sicherheitseinrichtungen werden regelmäßig auf ihre Betriebs- und Ausfallsicherheit überprüft.

Optional ist eine Zusammenarbeit mit externen Rechenzentren über Sub-Dienstleister möglich, diese stehen für den Testbetrieb, Redundanz-Konzepte (Geo-Redundanz) auf Anwendungsebene (durch Cluster, Trennung Rechenzentren, separate Daten-Spiegel etc.) auf Weisung zur Verfügung.

Für ein vollumfängliches Backup, je nach Zweckbindung der jeweiligen Verarbeitung, stehen unterschiedliche Archivierungsmöglichkeiten zur Verfügung, z.B. eine regelmäßige automatisch initiierte und überwachte Datensicherung (üblicherweise einmal pro Kalenderwoche eine Vollsicherung, tägliche

inkrementelle Sicherungen). Die normale Haltezeit dieser Sicherungen wird auf Weisung umgesetzt und im Leistungsschein dokumentiert. Die Datensicherung kann in einem separaten Backup-System, welches in einem anderen Brandschutzabschnitt oder an einem anderen Standort wie das Produktivsystem steht, erfolgen.

Auf allen Arbeitsplatzrechnern der Arvato Systems kommt ein Virenschutz zum Einsatz. Das Vorhandensein eines Virenschutzes, sowie die regelmäßige Aktualisierung des Virenpatterns wird durch den Einsatz einer zentralgesteuerte Client-Antivirus-/ und Firewall-Lösung sichergestellt.

Das zeitnahe Einspielen von Sicherheitsupdates für die genutzten Betriebssysteme und Anwendungsprogramme wird über entsprechende Group Policies vorgeschrieben und durch Überwachung des Patch-Levels sichergestellt.

Themen rund um das BCM (Business Continuity Management) sind in dem Kapitel Incident-Response-Management genauer beschrieben.

4.1.2 **Dienstleistungen ohne direkte RZ-Anbindung**

Eine Verarbeitung der Daten durch Mitarbeiter erfolgt über Remote / WLAN im relevanten Auftraggeberrechenzentrum und unterliegt somit auch der Verfügbarkeit dieses Rechenzentrums.

Sämtliche Mitarbeiter unterliegen der Anweisung, keine tätigkeitsrelevanten Daten auf dem Notebook zu speichern, sondern hierfür eingerichtete Backup-gesicherte Filebereiche zu nutzen, um das Risiko eines Verlustes der Daten auszuschließen.

4.1.3 **Public Cloud**

Es besteht ein Backup-Konzept. In diesen Dokumenten werden die Maßnahmen zur Sicherung von personenbezogenen und unternehmenskritischen Daten beschrieben.

Hierzu gehört eine regelmäßige vollständige Sicherung. Zudem werden in regelmäßigen Abständen und ggf. nach dem Aufsetzen neuer Datenverarbeitungsanlagen und nach tiefgreifenden Änderungen am Aufsatz einer Anlage, elektronische Abbilder von der jeweiligen Anlage erstellt.

Die Datensicherungen werden je nach Prozess oder Relevanz in weiteren Gebäuden oder extern ausgelagert. Eine unterbrechungsfreie Stromversorgung wird eingerichtet.

Im Übrigen bestehen entsprechende Notfall- und Business-Continuity-Pläne für Facilities des Cloudanbieters.

Auf Anfrage können Auszüge und Zusammenfassungen aus entsprechenden Konzepten zu entsprechenden Verfahren zur Verfügung gestellt werden.

4.2 Auftragskontrolle

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

4.2.1 **RZ-Outsourcing / (Virtual) Private Cloud / Dienstleistungen ohne direkte RZ-Anbindung**

Die Daten werden nur gemäß der Weisung des Auftraggebers verarbeitet. Diese Weisungen haben mindestens in Textform und ausschließlich durch berechtigte Personen des Auftraggebers an berechtigte Personen des Auftragnehmers zu erfolgen.

Alle Mitarbeiter sind auf das Datengeheimnis, sowie nach Spezialverpflichtungen wie z.B. das Fernmeldegeheimnis und das Sozialgeheimnis verpflichtet. Eine Einsichtnahme ermöglicht die Durchführung von stichprobenartigen Kontrollen.

Rechenzentrumsbesichtigungen oder Audits sind in den relevanten Rechenzentren nach der Verhältnismäßigkeit und rechtzeitiger schriftlicher Anmeldung beim verantwortlichen Fachbereich möglich. Die Organisation und Durchführung eines Audits unterliegt, zum Schutz der personenbezogenen Daten unterschiedlicher Verantwortlicher, der Auditrichtlinie.

4.2.2 **Public Cloud**

Der Dienstleister hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.

Mitarbeiter werden über ihre Rollen und Verantwortlichkeiten z.B. im Wege vorbereitender Schulungen instruiert. Der Auftraggeber hat einen oder mehrere Verantwortliche für die Kontrolle und das Monitoring der Datensicherheitsvorgaben benannt.

Es werden Dokumente zu Datenschutz- und Datensicherheit, Verantwortlichkeiten und relevanten Verfahren geführt und überprüft.

Die Konzernrevision (IT und kaufmännische Revision) führt innerhalb der verbundenen Unternehmen (gemäß Definition der §§15ff AktG) in regelmäßigen Abständen umfassende Kontrollen durch. Das Compliance Management führt innerhalb der verbundenen Unternehmen (gemäß Definition der §§15ff AktG) in regelmäßigen Abständen umfassende Kontrollen durch.

Mit externen Dienstleistern werden entsprechende Verträge abgeschlossen. Die Vertragsdurchführung wird durch entsprechende Kontrollen nachverfolgt und kontrolliert.

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

5.1 Datenschutzmanagement bei der Arvato Systems Group

Für sämtliche rechtliche Einheiten der Arvato Systems, in denen das Kerngeschäft die Durchführung von Verarbeitungsvorgängen mit personenbezogenen Daten oder besonderen per-

sonenbezogenen Daten gem. Artikel 9 DSGVO oder personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten gem. Artikel 10 DSGVO erfolgt, wurde ein externer Datenschutzbeauftragter bestellt. Als Ansprechpartner in den einzelnen rechtlichen Einheiten steht ein Team aus ausgebildeten Datenschutzbeauftragten, in der Funktion von Datenschutzkoordinatoren, unter der E-Mailadresse Datenschutz@arvato-systems.de, zur Verfügung.

Arvato Systems definiert die Eckpfeiler des Datenschutzes in der Konzerndatenschutzrichtlinie, sowie konkreter in der Arvato Systems internen Datenschutzrichtlinie.

Durch den Datenschutzbeauftragten und die IT-Revision werden in regelmäßigen Abständen Audits zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen durchgeführt. Im Rahmen der Verhältnismäßigkeit besteht nach rechtzeitiger Vorankündigung eine Kontrollmöglichkeit im Rahmen eines Audits durch den Auftraggeber.

Arvato Systems kann als Nachweis für eine sicherheitsrelevante Verarbeitung die folgenden Zertifizierungen nachweisen: ISO / IEC 27001.

Bei Arvato Systems kann ein ISAE-Report zum Nachweis einer ordnungsgemäßen Verarbeitung und der Beachtung der Informationssicherheit erworben werden.

Das Sicherheitskonzept der Arvato Systems ist in der Konzernrichtlinie zur Information-Security-Policy festgeschrieben.

Zur Erhöhung des Schutzniveaus bei der Verarbeitung von personenbezogenen Daten für den Betroffenen ist die interne Datenschutzrichtlinie der Arvato Systems mit genehmigten Verhaltensregeln für alle Mitarbeiter einzuhalten. Ebenfalls wird das Risiko durch ein wirksames Patch-Management, Pentests, Log-Analysen, Beschäftigung mit Websicherheit (z.B. OWASP) und über ein SOC-Center gewährleistet. Für die technisch organisatorischen Maßnahmen wird ein risikobasierter Ansatz präferiert.

Die Gewährleistung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technisch organisatorischen Maßnahmen und der Sicherheit der Verarbeitung erfolgt über den folgenden PDCA-Zyklus mit Plan (Entwicklung eines Sicherheitskonzeptes), Do (Einführung von TOMs), Check (Überwachung der Wirksamkeit / Vollständigkeit) und Act (Kontinuierliche Verbesserung).

Die Übermittlung personenbezogener Daten an ein Drittland erfolgt in Abstimmung zwischen dem Auftraggeber und dem Auftragnehmer unter Hinzuziehung von Standarddatenschutzklauseln.

Der Dienstleister gewährleistet in seinem eigenen Verantwortungsbereich eine vom Schutzniveau vergleichbare Umsetzung des Datenschutzmanagements wie Arvato Systems.

5.2 Incident-Response-Management bei der Arvato Systems Group

Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen rasch wiederherzustellen

Im Rahmen des etablierten BCM (Business Continuity Management) zur Sicherstellung des Geschäftsbetriebes während einer Notlage oder Großstörung sowie zur schnellstmöglichen Wiederherstellung aller für den Auftraggeber bereitzustellenden Dienste sind Verfahren dokumentiert. Es werden regelmäßig Wiederanlauf-Übungen durchgeführt.

Maßnahmen, welche die Belastbarkeit der Systeme und Dienste gewährleisten, sind so ausgelegt, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben. Themen rund um die Speicher-, Zugriffs- und Leitungskapazitäten, sowie zu Backup und Redundanz-Konzepten sind in der Verfügbarkeitskontrolle detaillierter aufgenommen.

5.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) bei der Arvato Systems Group

Die Umsetzung des Datenschutzes wird bei der Produktentwicklung durch die Berücksichtigung eines internen White Paper „Datenschutz in der Produktentwicklung“, sowie einer Checkliste zur Berücksichtigung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen begleitet.

Die Nutzung des White Papers ist in der Datenschutzrichtlinie von Arvato Systems zwingend vorgegeben.