Technisch-organisatorische Maßnahmen (TOMs) zur Datensicherheit

Dokumentation DO0020 - Rev.: 2.3

Inhaltsverzeichnis

Technisch-organisatorische Maßnahmen (TOMs) zur Datensicherheit

Dokumentation DO0020 - Rev.: 2.3

1 Zielsetzung

Dieses Dokument beschreibt die technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO.

2 Geltungsbereich

Dieses Dokument gilt ab dem 01.05.2024 für alle deutschen Paragon-Standorte:

- Paragon Germany GmbH, Gutenbergstraße 3-5, 92421 Schwandorf
- Paragon Germany GmbH, Betriebsstätte Korschenbroich, Mühlenstraße 57, 41352 Korschenbroich
- Paragon Germany GmbH, Betriebsstätte Magdeburg, Marienstraße 1, 39112 Magdeburg
- Paragon Germany GmbH, Betriebsstätte Weingarten, Josef-Bayer-Straße 5, 88520 Weingarten

3 Einführung

Dieses Dokument beschreibt die technischen und organisatorischen Sicherheitsmaßnahmen, die von Paragon zum Schutz von Informationen implementiert wurden, und es ist auf alle von Paragon bereitgestellten Services, Standorte, verwalteten Systeme sowie auf seine Mitarbeiter[1], Partner und Dritte anwendbar.

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

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

4.1 Zutrittskontrolle

Definition: Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, verwehrt wird.

1. Alle Außentüren der Betriebsgebäude sind verschlossen. Ein Zutritt zu den Geschäftsräumen ist nur den zutrittsberechtigten Personen möglich, Dritten nur in Begleitung eines Mitarbeiters.
2. Alle Besucher der Standorte der Paragon werden mit Datum und Uhrzeit ihres Betretens und Verlassens von den Mitarbeitern am Eingangsbereich erfasst.
3. Für die Vergabe von Berechtigungen an Mitarbeiter sind die Vorgesetzten zuständig. Die Einrichtung der Zutrittsberechtigungen und deren Entzug erfolgt zentral und revisionssicher durch die örtliche Personalsachbearbeitung oder durch das Facility Management.
4. Es existieren Zutrittsregelungen für betriebsfremde Personen (z. B. Wartungs- und Reinigungspersonal, Besucher, Dienstleister). Als betriebsfremd gelten Personen, die nicht dauerhaft wiederkehrend für Paragon tätig sind. Diese und andere fremde Personen dürfen nur in Begleitung von berechtigten Mitarbeitern die Sicherheitsbereiche betreten. Jeder betriebsfremde Dritte wird in Schriftform auf den Datenschutz und zur Geheimhaltung verpflichtet, in Listen mit der Registrierung der

[1] Zur besseren Lesbarkeit wird in diesem Dokument das generische Maskulinum verwendet. Die verwendeten Personenbezeichnungen beziehen sich - sofern nicht anders kenntlich gemacht - auf alle Geschlechter.

Besucherausweisnummer / Token-Nummer, der besuchten Person und dem Zeitraum erfasst und erhält einen deutlich erkennbaren Besucherausweis / Zugangstoken.

5. Die Authentisierung der Zutrittsberechtigung erfolgt durch ein elektronisches Zutrittskontrollsystem. Die Zutrittsberechtigungen sind im System hinterlegt, werden über Token gesteuert und unterliegen einer regelmäßigen Prüfung.
6. Der Zutritt zu den Serverräumen und IT-Räumen ist nur einem definierten und ausdrücklich berechtigten Personenkreis möglich. Zusätzlich wird der Zutritt durch eine Zwei-Faktor-Authentisierung geschützt. Alle Serverräume und IT-Räume sind durch eine Alarmanlage gesichert.
7. Die Rechenzentren in Frankfurt sind durch die Verwendung von Spezialfenstern und Sicherheitsschlössern vor weiteren Zutrittsmöglichkeiten gesichert.
8. Zentrales IT-Equipment wie Switches, Router sowie Server ist in zutrittsgesicherten Serverräumen und IT-Räumen untergebracht.
9. Es gibt für die Betriebsgebäude abgestufte Sicherheitszonen (Zwiebelschalenprinzip) und damit verbunden dedizierte Zutrittsberechtigungen. Die Berechtigung für die einzelnen Zonen werden entsprechend dem Need-to-know- / Minimalprinzip vergeben.
10. Alle Zutritte werden elektronisch protokolliert, sodass überprüft werden kann, wer zu welchem Zeitpunkt wo Zutritt hatte. Das Zutrittskonzept lässt es zu, den Zutritt für jeden Bereich und jeden Mitarbeiter im Detail (zeit- und personengebunden) zu regeln.
11. Die Betriebsstätten werden außerhalb der Geschäftszeiten durch eine Alarmanlage oder durch regelmäßige Rundgänge des Sicherheitspersonals gesichert. Die Alarmmeldungen gehen direkt an Sicherheitsunternehmen, die unmittelbar einen definierten Personenkreis informiert, der die weiteren, im Einzelfall gebotenen Maßnahmen definiert.
12. Die Betriebsstätten sind zur Sicherung kameraüberwacht. Die Videos werden maximal für 72 Stunden gespeichert.
13. Die Einhaltung der Zutrittsschutzmaßnahmen werden im Rahmen interner Audits und Regelkontrollgängen von Datenschutzkoordinatoren, von Mitarbeitern der Informationssicherheit und vom Facility Management oder den für den Zutritt verantwortlichen Personen überwacht.

4.2 Zugangskontrolle

Definition: Die Zugangskontrolle gewährleistet, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -verfahren gehindert werden.

1. Die PC-Arbeitsplätze (Laptops / Notebooks, Desktop-PCs) sind zugangsgeschützt. Benutzer können auf gespeicherte Dateien nur zugreifen oder Daten nur speichern, sofern sie dafür über das Active Directory berechtigt sind.
2. Vergabe und Entzug von Zugangsberechtigungen wird über den Starter-/Mover-/Leaver-Prozess realisiert. Weiterhin finden zyklische Reviews auf die Notwendigkeit der Berechtigungen statt. Diese finden mindestens einmal pro Jahr statt.
3. Die persönlichen Passwörter aller Mitarbeiter sind mindestens 12-stellig, und beinhalten mindestens Zeichentypen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Aufgrund des hinreichend komplexen Passwortes wird gemäß den Empfehlungen vom BSI bzw. NIST kein monatlicher Passwortwechsel mehr erzwungen. Ein Passwortwechsel ist nach spätestens 120 Tagen unvermeidlich. Nach fünfmaliger Falscheingabe wird das Benutzerkonto gesperrt und kann nur durch einen Administrator

wieder freigeschaltet werden. Das Mindestalter des Passwortes beträgt einen Tag und es darf für 13 Iterationen nicht wiederverwendet werden.

4. Zur Anmeldung / Identifizierung im System muss der Benutzer seine User-ID und sein persönliches Passwort eingeben. Im Active Directory sind die Zugangsberechtigungen hinterlegt, wobei der Zugriff auf die DV-Systeme selbst nur durch dafür berechtigte und autorisierte Personen erfolgen kann (Administratoren). Sämtliche Zugänge (erfolgreiche und abgewiesene) werden protokolliert.
5. Die Accounts inaktiver Benutzer werden nach einem fest definierten Zeitraum gelöscht, wenn das Passwort nicht regelmäßig gewechselt wird.
6. Es werden für die einzelnen Ebenen unterschiedliche Teams eingesetzt, die lediglich Zugriff auf die von diesen Mitarbeitern verantworteten Komponenten haben. So existieren beispielsweise unterschiedliche Teams für den Betrieb der Virtualisierungslösungen, des Netzwerks und der Windows- bzw. Unix-Administration mit unterschiedlichen Berechtigungen.
7. Der Internet-Zugang und das interne Netzwerk sind gegen ungewollte Zugriffe von außen durch den Einsatz von Firewalls und mittels Netzwerksegmentierung abgeschottet.
8. Die Netzwerksegmentierung basieren auf einem oder mehreren Netzwerken mit unterschiedlichen Sicherheitslevel, physikalisch (z. B. L2 Switch) oder auch logisch (VLANs) getrennt, zwischen denen nur mittels Firewall Daten kontrolliert ausgetauscht werden können.
9. Telearbeit bzw. mobiles Arbeiten ist lediglich unter Verwendung eines VPNs mit einer Multi-Faktor-Authentifizierung (Authenticator-App in Kombination von einem Benutzernamen und Passwort) möglich.
10. PC-Arbeitsplätze werden beim Verlassen gesperrt. Mittels zentraler Domain Policies ist festgelegt, dass die Sperre des Arbeitsplatzes nach 5 Minuten Inaktivität des PC-Arbeitsplatzes automatisch erfolgt.
11. Eine Anti-Malware-Lösung wird auf Servern und Endgeräten eingesetzt. Die Lösung dient der automatischen Identifizierung und Priorisierung von Bedrohungen auf Endgeräten und Servern, und dient der Malware-Erkennung und -Beseitigung (Anti-Virus-Schutz). Die Anti-Malware-Lösung wird mindestens einmal täglich mit den neusten Signaturen (wie z. B. Anti-Viren) versehen.
12. Ein Secure Mail Gateway (SMG) fungiert als zentrale Schnittstelle für alle eingehenden und ausgehenden E-Mails, um vor unerwünschten Nachrichten zu schützen, darunter Spam, Phishing-Angriffe und Malware.

4.3 Zugriffskontrolle

Definition: Die Zugriffskontrolle gewährleistet, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und diese nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1. Benutzerkonten ermöglichen auf Grundlage definierter Rollen (Role-Based Access Control [RBAC]) den Zugang auf Systeme und Zugriff auf Daten. Zugangs- und Zugriffsrechte werden mit bestimmten Rollen und nicht mit einzelnen Benutzern verknüpft; einzelnen Benutzern wird eine Rolle zugewiesen.
2. Die Zugriffskontrolle erfolgt durch Benutzerkennungen und Passwörter. Ein Zugriff auf die Server ist nur mit gesonderter Authentifizierung der Benutzer möglich; es existieren getrennte Benutzerkonten für Administratortätigkeit und Sachbearbeitung. Jeder Mitarbeiter erhält nur die Berechtigungen, die für die Erfüllung seiner Tätigkeit notwendig sind (auf Basis der Prinzipien „need-to-know“ und „least privilege“). Die personenbezogene Authentifizierung erfolgt durch die Zugangskontrolle.
3. Das Identity & Access Management besteht aus einem Verzeichnisdienst für die zentrale Verwaltung von internen Identitäten. Es liefert die Datenbasis für die untergeordnete Active Directory-Implementierung.

4. Hinterlegte Notfallpassworte.

4.4 Trennungskontrolle

Definition: Das Trennungsgebot gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

1. Über den gesamten Produktionsprozess ist jederzeit gewährleistet, dass jeder Datensatz jedem Mandanten logisch zugeordnet werden kann.
2. Neben der produktiven Umgebung existiert eine Staging-Umgebung für Tests sowie Entwicklungsumgebungen.
3. Auf den Testsystemen (Staging) werden keine Produktiv- bzw. Echtdaten gespeichert (z. B. Verwendung der Echtdaten auf den Testsystemen zu Testzwecken), es sei denn, es liegt eine explizite Anforderung oder Genehmigung des Kunden vor.
4. Separate Jobs im Pre-Processing. Jedes Dokument bleibt über den gesamten IT-Aufbereitungs- und Produktionsprozess eindeutig zuordenbar. Durch IT-gestützte Kuvertierung wird sichergestellt, dass Sendungen jederzeit empfängergetrennt verarbeitet werden.

4.5 Pseudonymisierung und Verschlüsselung

Definition: Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

1. Das Verfahren zur Verschlüsselung des Datenaustausches wird mit dem Kunden abgestimmt festgelegt.
2. Es wird ein zertifizierter Trustcenter-Dienst, dessen „Certification Authority“ (CA) in allen gängigen Webbrowsern als vertraute Root CA gelistet ist, genutzt. Das Trustcenter ist gemäß ETSI TS 102 042 resp. EN 319 411-1, ISO/IEC 27001, BSI TR-03145 „Secure Certification Authority Operation" als vertrauter Service Provider zertifiziert. Im Rahmen der Trustcenter Services werden Benutzerzertifikate für „S/MIME“-E-Mail-Verschlüsselung und E-Mail-Signatur, Gerätezertifikate für die sichere Authentifizierung sowie TLS-Server-Zertifikate beschafft und gepflegt.
3. E-Mails werden bei Bedarf Ende-zu-Ende-verschlüsselt.
4. Eine Datenträgerverschlüsselung wird auf allen Laptops / Notebooks und Smartphones eingesetzt. Diesbezüglich kommen unterschiedliche Lösungen wie z. B. Bitlocker oder die Datenträgerverschlüsselung von Apple zum Einsatz.
5. Eine Pseudonymisierung der Daten muss vom Auftraggeber selbst durchgeführt werden, da nur der Eigentümer der Daten diese in geeigneter Form verändern darf. Nur mit der Zustimmung des Eigentümers kann der Auftragnehmer die Pseudonymisierung übernehmen (kostenpflichtig).

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

5.1 Weitergabekontrolle

Definition: Die Weitergabekontrolle gewährleistet, dass Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1. Für die abgesicherte Datenübermittlung zwischen Kunden und Auftragnehmer werden verschlüsselte Datenübertragungswege z. B. per sFTP oder VPN eingesetzt. Maßgebend ist die Kundenanforderung im Einzelfall, die ausdrücklich schriftlich erklärt werden muss.
2. Die Datenlöschung im Bereich Print erfolgt automatisiert höchstens 30 bis 90 Tage nach Auftragsende – es sei denn, eine ausdrückliche Kundenanforderung bedingt eine abweichende Löschfrist.
3. Die Verwendung von Massenspeichermedien an Laptops / PCs wird technisch durch die Sperre der entsprechenden Ports (z. B. USB) am Gerät unterbunden; Ausnahmen werden geprüft und das Ergebnis der Überprüfung dokumentiert.
4. Es werden nur freigegebene Umgebungen für den Dateiaustausch mit externen Stellen verwendet und die dortige Übermittlung protokolliert. Maßgebend ist die Kundenvorgabe im Einzelfall.
5. Zugriff aufs Firmennetzwerk ist nur mit firmeneigener Hardware erlaubt und bei mobiler Arbeit nur über VPN mit Multi-Faktor-Authentifizierung (MFA) möglich.
6. Alle Datenübertragungen werden protokolliert. Bei Dateneingang wird die Datenübertragung auf ihre Vollständigkeit hin überprüft.
7. Die Datenträgervernichtung erfolgt kontrolliert durch einen zugelassenen und zertifizierten Entsorger bzw. vor Ort durch eine Industrieschredderanlage.
8. Die datenschutzkonforme Löschung und Entsorgung von Datenbeständen auf Datenträgern erfolgen gemäß DIN 66399. Die Regelung zur datenschutzgerechten Vernichtung von Daten bzw. Datenträgern wird durch interne Sicherheitsschulungen in regelmäßigen Abständen realisiert.
9. In den Bürogebäuden stehen auf jeder Etage, in der Regel in jedem Flügel, Entsorgungscontainer für Papier.
10. Die Datenübermittlung innerhalb der Produktionsstandorte erfolgt in gesicherten Bereichen der Paragon.

5.2 Eingabekontrolle

Definition: Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

1. Protokollierung der Datenaufbereitung (soweit Veränderungen am Content vertraglich vereinbart wurden).
2. Definierte Aufbewahrungsfristen von Systemlogs/-ereignissen zu Nachweiszwecken.
3. Die lokale Protokollfunktion ist auf allen relevanten IT-Systemen und Netzwerkgeräten aktiviert. Protokolldaten von kritischen Systemen werden an das SIEM-System übermittelt. Die Protokolldaten werden im SIEM-System für 90 Tage gespeichert und für weitere 90 Tage in dem SIEM-Backup-Systemen vorgehalten.
4. Durch die Übertragung von relevanten Protokolldaten an ein zentrales System wird sichergestellt, dass die Protokolldaten nicht verändert werden können.
5. Eine Komponente des SIEM-Systems überprüft die Protokolldaten in Echtzeitanalyse. So erfolgt eine Alarmierung des Security Operations Center (SOC), sofern ungewöhnliche Aktivitäten erkannt werden.

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

6.1 Verfügbarkeitskontrolle

Definition: Die Verfügbarkeitskontrolle gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

1. Eine Notstromversorgung wichtiger IT-Systeme ist gewährleistet.
2. Die Vorschriften zum Brandschutz werden beachtet und eingehalten, im Rahmen von Brandschutzbegehungen überprüft und die hier gemachten Auflagen umgesetzt. In allen Räumen herrscht Rauchverbot.
3. Auf außerhalb der Arbeitszeiten geschlossene Fenster, gesicherte Türen und dem aufgeräumten Arbeitsplatz ist von allen Mitarbeitern zu achten. Jeder Mitarbeiter hat in seinem Bereich für die Sicherung des Arbeitsplatzes und des Gebäudes zu sorgen.
4. Alle Bereiche wie Serverraum, Produktionsräume und Büros sind brandschutzgesichert mit Feuer- und Rauchmeldeanlagen sowie Feuerlöschgeräten. Es besteht eine Alarmaufschaltung zur Feuerwehr.
5. Regelmäßige Sicherung der zur Verarbeitung der Daten erforderlichen Programme und Skripte.
6. Klimatisierte und temperaturüberwachte Server- bzw. IT-Räume.
7. Anti-Malware-Lösung.
8. Kontinuierliche Lizenzüberwachung zur Vermeidung von Ausfällen systemkritischer Systeme.
9. Ein Notfallhandbuch inklusive der zu ergreifenden Sofortmaßnahmen ist erstellt.
10. Das Computer Security Incident Response Team (CSIRT) reagiert auf erkannte Sicherheitsvorfälle (Information Security Incident Response) und unterstützt im Bedarfsfall die forensische Analyse solcher Ereignisse.

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

7.1 Auftragskontrolle

Definition: Die Auftragskontrolle gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

1. Die Mitarbeiter werden regelmäßig im Bereich Datenschutz und Informationssicherheit geschult. Alle Mitarbeiter verpflichten sich vor Beginn der Auftragsverarbeitung auf unsere Geheimhaltungs-, Datenschutz- und Informationssicherheitsvorgaben, der Verpflichtungserklärung.
2. Ein Zugriff auf Endkundendaten der Auftraggeber durch Subdienstleister ist nur innerhalb Deutschlands möglich; auf restliche Daten der Auftraggeber nur innerhalb der EU.
3. Mit allen relevanten Dienstleistern besteht ein Vertrag gem. Art. 28 DSGVO, welcher sämtliche Anforderungen der Auftraggeber weitergibt; die Mitarbeiter des Dienstleisters, die Zugriff auf Daten des Auftraggebers haben, sind auf das Datengeheimnis / Vertraulichkeit verpflichtet.
4. Es besteht ein Verfahren zur Dienstleister- / Lieferantenauswahl und -bewertung. Lieferanten und Dienstleister sind regelmäßig zu bewerten; bei hohem Risiko zumindest einmal jährlich.

5. Die Kontrolle der technischen und organisatorischen Maßnahmen bei Subunternehmern erfolgt durch das Datenschutz- und Informationssicherheitsteam. In der Regel wird dabei zwischen einem Vor-Ort-Audit und einer Prüfung auf Unterlagen-/ Selbstauskunftsbasis gewechselt.
6. Bei Fehlern hinsichtlich der Datenverarbeitung oder Verstoß gegen den Datenschutz sowie IT-Sicherheitsvorfällen erfolgt eine unverzügliche Information an die im Vertrag mit dem Auftraggeber benannte Stelle.
7. Ausgewählte Server- und Client-Systeme sind in ein Schwachstellenmanagement-System integriert und werden regelmäßig auf Schwachstellen geprüft. Diese prüfen den Stand der Sicherheitsupdates durch authentifizierte Scans. Entsprechende Erkenntnisse fließen in die Patch-Prozesse ein. Weiterhin werden zyklisch externe Penetrationstests ausgewählter Anwendungen durchgeführt (i. d. R. jährlich).
8. Die mit der Auftragsbearbeitung befassten Mitarbeiter werden auf die Auftragsspezifikation des Auftraggebers hingewiesen. Das schließt die spezifizierten Arbeitsanweisungen mit ein.
9. Sämtliche Verträge und Auftragsbestätigungen liegen vor und enthalten alle Pflichten, Aufgaben und Vorgaben von Auftraggeber und Auftragnehmer.
10. Der Auftraggeber kann Personen / Stellen benennen, die Weisungen zu Aufträgen erteilen dürfen. Der Auftragnehmer verpflichtet sich dann, dass nur von diesen Personen / Stellen Weisungen entgegengenommen werden.

7.2 Managementsysteme

Definition: Das bei Paragon integrierte Managementsystem (IMS) ist gekennzeichnet durch die Zusammenführung dreier Managementsysteme (ISO 9001, ISO 14001 & ISO/IEC 27001) in ein ganzheitliches System. Die Synergien, die durch das IMS entstehen, schärfen den Blick für Chancen und Risiken im Unternehmen.

1. Aktive Unterstützung von Datenschutzpolitik und Datenschutzzielen durch die Geschäftsführung.
2. Etabliertes Datenschutzmanagement-, ISO-9001-Qualitäts- und ISO-/IEC-27001-Informationssicherheits-Managementsystem. Das Qualitätsmanagement- und das Informationssicherheits-Managementsystem (ISMS) wurden und werden weiterhin von Auditoren bewertet und erhalten regelmäßig eine Zertifizierung gemäß ISO 9001:2015 bzw. ISO/IEC 27001:2022.
3. Regelmäßige Überprüfung der technischen und organisatorischen Sicherheitsmaßnahmen.
4. Kontinuierlicher Verbesserungsprozess.
5. Datenschutz- und informationssicherheitsrelevante Richtlinien, Standards und Prozesse.
6. Kontinuierliche Datenschutz- und Informationssicherheitsschulungen der Mitarbeiter (eLearning, persönlich, Mitarbeiter-Zeitschrift)

Paragon verfügt über eine etablierte Informationssicherheitsfunktion, die vom Head of Information Security, IKS & BCM geleitet wird. Die Funktion ist dafür verantwortlich, die Implementierung von Informationssicherheitselementen wie Framework, Richtlinien, Prozesse und Konformitätsmaßnahmen sicherzustellen.

Der Head of Information Security, IKS & BCM stimmt sich mit dem Datenschutzbeauftragten in Bezug auf die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten ab.

Der Auftragnehmer gewährt dem Auftraggeber auf dessen Wunsch die Einsicht in sein umfassendes und aktuelles Datenschutz- und Informationssicherheitskonzept für diese Auftragsdatenverarbeitung.

8 Mitgeltende Dokumente

Alle auf der Leitlinie LL0017 „Informationssicherheit und BCM“ basierenden Informationssicherheitsrichtlinien, wie in der Dokumentation DO0331 „Übersicht Dokumente für Informationssicherheit und BCM“ dargestellt, sowie die Leitlinie Informationssicherheit und BCM selbst.