Deloitte.



Deloitte TOMs

Technische und organisatorische Maßnahmen

Mandantenversion, 01.11.2025

Deloitte.

Technische und organisatorische Maßnahmen (TOMs) und deren Kontrolle durch den Auftragnehmer

Die **Deloitte Deutschland GmbH Wirtschaftsprüfungsgesellschaft** sowie die **Deloitte Legal Rechtsanwaltsgesellschaft mbH** und alle in Deutschland mit ihnen verbundenen Unternehmen erheben, verarbeiten oder nutzen selbst oder im Auftrag personenbezogene Daten und haben hierzu die folgenden technischen und organisatorischen Maßnahmen getroffen, um die Ausführung der Vorschriften der Datenschutz-Grundverordnung (DSGVO) sicher zu stellen.

Die hier beschriebenen Maßnahmen gelten für alle von der **Deloitte Deutschland GmbH Wirtschaftsprüfungsgesellschaft** sowie die **Deloitte Legal Rechtsanwaltsgesellschaft mbH** betriebenen oder eingesetzten Systeme und Dienste, welche Daten speichern oder verarbeiten. Die Verantwortung für die im Rahmen einer Auftragsverarbeitung zu treffenden Schutzmaßnahmen hat aber jedes Unternehmen für die von ihm verwalteten Systeme und Informationen selbst zu tragen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technologischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei dürfen die festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen werden nachgehalten und dokumentiert. Die vertraglich vereinbarten Regelungen zum Datenschutz bleiben davon unberührt.

Ein adäquater Schutz von Informationen kann in vielen Fällen nur über eine Kombination verschiedener Maßnahmen erreicht werden.

Rückfragen zu den im Folgenden erläuterten technischen und organisatorischen Maßnahmen können Sie gerne direkt an security@deloitte.de richten.

Deloitte.

Inhaltsverzeichnis

1 PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG PERSONENBEZOGENER DATEN (ART. 32 ABS. 1 LIT. A DSGVO) 4

1.1 Maßnahmen zur Pseudonymisierung 4

1.2 Maßnahmen zur Verschlüsselung 5

2 VERTRAULICHKEIT, INTEGRITÄT UND BELASTBARKEIT DER SYSTEME UND DIENSTE (ART. 32 ABS. 1 LIT. B DSGVO) 6

2.1 Maßnahmen zur (physischen) Zutrittskontrolle 6

2.2 Umsetzung der Zugangskontrolle 7

2.3 Maßnahmen zur Zugriffskontrolle (Berechtigungsmanagement) 8

2.4 Maßnahmen zur Eingabekontrolle 9

2.5 Maßnahmen zur Trennungskontrolle 9

2.6 Maßnahmen zur Weitergabekontrolle 10

2.7 Maßnahmen zur Belastbarkeit 10

3 VERFÜGBARKEIT UND WIEDERHERSTELLUNG DER SYSTEME UND DIENSTE (ART. 32 ABS. 1 LIT. C DSGVO) 11

3.1 Maßnahmen zur Verfügbarkeit (Sicherung) 11

3.2 Maßnahmen zur Löschung 11

3.3 Recovery measures 12

4 VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER WIRKSAMKEIT DER TOMS (PDCA-ZYKLUS) (ART. 25 ABS. 1 DSGVO) 13

4.1 Maßnahmen zur Auftragskontrolle (Art. 28, 25 Abs. 1 DSGVO) 13

4.2 Maßnahmen zur Ausführung / Umsetzung 14

5 DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN (ART. 25 ABS. 2 DSGVO) 15

5.1 Maßnahmen für datenschutzfreundliche Voreinstellungen 15

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

1.1 Maßnahmen zur Pseudonymisierung

Pseudonymisierung wird die Verarbeitung personenbezogener Daten genannt, wenn diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer/mehreren spezifischen betroffenen Person(en) zugeordnet werden können. Die zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen technischen und organisatorischen Maßnahmen, die gewährleisten, dass die personenbezogenen Daten nicht oder nur mit erheblichem Aufwand einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können (Art. 32 Abs. 1 lit. a) DSGVO. Eine Pseudonymisierung wird bei Bedarf für alle zu verarbeitenden personenbezogenen Daten ab hohem Schutzbedarf oder Daten mit anderweitig identifizierten Risiken durchgeführt.

Technische Maßnahmen	Organisatorische Maßnahmen
• Errechnung von Hashwerten von den identifizierenden Daten (keine Speicherung einer Zuordnungsliste). • Trennung der Identifikationsmerkmale von den Daten und Speicherung in getrennten Systemen. Sofern eine Zuordnung erforderlich ist, erfolgt diese nur noch über Zuordnungstabellen.	• Der Zugriff auf personenbezogene Daten und den Zusatzinformationen wird über ein differenziertes Berechtigungskonzept geregelt und dokumentiert. • Regelmäßige Schulung aller Mitarbeiter (mind. jährlich). • Die Verarbeitung von Identifikationsdaten wird über einen Autorisierungsprozess geregelt. • Personenbezogene Daten werden im Falle einer Weitergabe (oder nach Ablauf der gesetzlichen Löschfrist) anonymisiert oder pseudonymisiert.

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

1.2 Maßnahmen zur Verschlüsselung

Ziel der Verschlüsselung ist es, den Schutz der Daten bei der Speicherung und beim Transport sicherzustellen. Die Verschlüsselung entspricht aktuellen Industriestandards und wird mindestens jährlich oder bei Bedarf, z. B. Änderungen der Designs oder Standards, überprüft und angepasst, um einen angemessenen Schutz zu gewährleisten (Art. 32 Abs. 1 lit. a).

Technische Maßnahmen	Organisatorische Maßnahmen
Die Speicherung und Übermittlung personenbezogener Daten erfolgt immer verschlüsselt auf allen Systemen, wie • Client (NB, PCs, Workstations), • Server, • Mobile Endgeräte (Tablet, Handys), • Mobilen Datenträgern (HDs, SSDs, USB-Sticks, ...), • Datenbanken, • Mails, • Passwörter. Dabei werden folgende Optionen verwendet: • Bitlocker oder FileVault zur Verschlüsselung von NBs, PCs, MACs mit 256-bit AES-Standard, • „data at rest“ Verschlüsselung von Datenbanken, • „data-in-transit“ Verschlüsselung mittels 2048-bit RSA-Verschlüsselung und SHA2 Signatur, • SFTP nach FIPS 140-2 Standard, • Verschlüsselung ext. Datenträger (HD, SSD, ext. Festplatten, ...) mit Bitlocker und PIN, • Verschlüsselung von E-Mails mittels TLS 1.3 zusammen mit AIP (Azure Information Protection), bei streng vertraulichen Daten mit S/Mime, PGP oder anderen, • Verschlüsselung von USB-Sticks, • Verschlüsselung von Webseiten per SSL, • Winzip nach FIPS 140-2 Standard, • Keine Übermittlung von Passwörtern im Klartext.	• Dokumentation und Sicherung aller Schlüssel, • Richtliniendokument zur Verschlüsselung, • Regelmäßige Schulung aller Mitarbeiter (mind. jährlich)

2 Vertraulichkeit, Integrität und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Maßnahmen zur (physischen) Zutrittskontrolle

Sicherheitsmaßnahmen, die den physischen und/oder logischen Zugang zu bestimmten Bereichen wie Gebäuden, Räumen oder Daten erlauben, um sicherzustellen, dass nur autorisierte Personen oder Systeme eintreten und auf Informationen zugreifen können.

Technische Maßnahmen	Organisatorische Maßnahmen
• Alarmanlagen mit Alarmaufschaltung des Erdgeschosses sowie sensibler Bereiche sind vorhanden. • Außentüren verfügen nur über einen Knopf und keinen Knauf zum Öffnen. • Die Ausgabe von Ausweisen, Chips oder Transpondern erfolgt nur nach definierten Sicherheitsrollen. • In den Erdgeschossen und in allen sensiblen Bereichen sind einbruchhemmende Fenster und Türen eingebaut. • Räume/Zonen sind immer gesichert und verschließbar. • Fenster Türen, Schachtabdeckungen, Aufzugs- und Filteranlagen werden gesichert. • Es werden sichere Schließsysteme mit dokumentierter Schlüsselverwaltung eingesetzt. • Sichtbares Tragen eines Dienst-, Gast-, oder Mitarbeiterausweises (mit Lichtbild) ist verpflichtend. • Sensible Bereiche, wie Empfang, RZ, Archive, Garage, werden videoüberwacht oder mit Bewegungsmeldern ausgestattet. • Aktivitäten an Zugangskontrollsystemen oder Vereinzelungsanlagen mit Ausweisleser werden protokolliert.	• Während der Betriebszeiten ist Empfangspersonal vor-Ort. • Es erfolgt eine Protokollierung aller ein- und ausgehenden Personen. • Es erfolgt eine Protokollierung der Zu- und Abgänge in sensiblen Bereichen, wie RZ, Archiv und anderen sensiblen Bereichen im Besucherbuch. • Die Auswahl von Reinigungs- und Wachpersonal erfolgt anhand von definierten Sicherheitsvorgaben. • Die Einteilung von Sicherheitszonen erfolgt gemäß ihrem definierten Risiko (z. B. RZ, Archive, Lager, ...) in den Bauplänen. • Ein Wachdienst ist vor Ort außerhalb der Betriebszeiten. • Es existieren Zutrittsregelungen für Ausnahmesituationen (z. Bsp. *Ausfall des Zutrittskontrollsystems, Katastrophenfall*, ...).

2 Vertraulichkeit, Integrität und Belastbarkeit der Systeme und Dienste
(Art. 32 Abs. 1 lit. b DSGVO)

2.2 Umsetzung der Zugangskontrolle

Die Maßnahmen der Zugangskontrolle regeln, welcher Nutzer Zugang zu einem IT-System, Laufwerk, Dateiordner etc. erhält.

Technische Maßnahmen	Organisatorische Maßnahmen
• Eine Anmeldung erfolgt immer über MFA, mittels Benutzerkennung und Passwort oder biometrischer Erkennung, Token, Authenticator PIN. • Automatische Sperrung der Systeme und Applikationen nach Zeit/Sitzungsende. • Anti-Virus Software auf allen Endgeräten. • Berechtigungskonzept für IT-Applikationen/IT-Systeme. • Einsatz von BIOS-Passwörtern für Endgeräte. • Einsatz von Gateway- und Firewall Systemen. • Einsatz von IDS- und IPS-Systemen. • Identifikation des Benutzers erfolgt immer über verschiedene Optionen, wie Authenticator PIN, biometrische Erkennung, Chipkarte oder Passwort. • Makros in Office Dokumenten sind standardmäßig deaktiviert. • MFA ist verpflichtend bei Systemen, die schutzbedürftige Daten, insbesondere Daten mit Personenbezug verarbeitet. • Passwortregelung nach BSI, NIST und ENISA – mit 3 von 4 Sets (groß, klein, Sonderzeichen und Zahlen) – für Standardbenutzer (mind. 10 Zeichen) – privilegierte Benutzer (mind. 16 Zeichen) – Sperrung nach 5 Fehlversuchen. • Sperrung und Überwachung externer Schnittstellen mittels DLP. • Verschlüsselung aller Datenträger und Netze. • Verwendung starker Passwörter, die nach Stand der Technik nur gehashed gespeichert werden. • VPN-Nutzung für Fernzugriffe / Remote Work.	• Ein Berechtigungskonzept und Geräteverwaltung für IT-Endgeräte (MDM) existiert. • Protokollierung aller Zugriffe auf IT-Systeme und Applikationen.

2 Vertraulichkeit, Integrität und Belastbarkeit der Systeme und Dienste
(Art. 32 Abs. 1 lit. b DSGVO)

2.3 Maßnahmen zur Zugriffskontrolle (Berechtigungsmanagement)

Die Zugriffskontrolle bezeichnet die Kontrolle dessen, welcher Nutzer bestimmte Daten verarbeiten darf. Dabei ist der Begriff „Verarbeitung“ i. S. v. Art. 4 Nr. 2 DSGVO sehr weit zu verstehen und umfasst jeden Vorgang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Technische Maßnahmen	Organisatorische Maßnahmen
• Anwendungsschutz durch Passwortsicherung. • Protokollierung von Zugriffen jedweder Art und Zugriffsversuchen mit definierten Aufbewahrungsfristen (mind. 90 Tage). • Regelmäßige, anlassbezogene sowie stichprobenartige Kontrollen der Zugriffsprotokolle. • Regelmäßige Kontrolle normaler und privilegierter Berechtigungen (mind. jährlich).	• Begrenzung der Anzahl von Administratoren. • Definition eines Zugriffskonzepts über definierte Rollen (RBAC). • Definition individueller Applikations-, System-, und Dienstberechtigungen basierend auf dem Rollenmodell. • Schulung der Administratoren. • Umgehende Anpassung von Berechtigungen bei Austritt oder Wechsel von Mitarbeitern. • Vergabe differenzierter Zugriffsberechtigungen (Lesen/Schreiben/Ändern/Löschen). • Zweckgebundene Berechtigungsvergabe nach dem Minimalprinzip (Need to know) im Vier-Augenprinzip mit den geringsten Rechten (Least Privilege).

2 Vertraulichkeit, Integrität und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO)

2.4 Maßnahmen zur Eingabekontrolle

Die Eingabekontrolle dient der Nachvollziehbarkeit, wer wann welche personenbezogenen Daten in einem System eingegeben, verändert oder gelöscht hat. Ziel ist es, nachträglich eine Überprüfbarkeit zu gewährleisten und die Verantwortlichkeit für Datenänderungen festzustellen. Typische Maßnahmen sind die Protokollierung aller Datenaktionen und die Sicherung dieser Protokolle, um sie später auslesen und überprüfen zu können.

Technische Maßnahmen	Organisatorische Maßnahmen
• Protokollierung der Dateneingaben.	• Organisatorisch festgelegte Zuständigkeiten für Eingaben. • Regelmäßige Auswertung von Logs. • Versionierung aller relevanten Dokumente.

2.5 Maßnahmen zur Trennungskontrolle

Die personenbezogenen Daten des Auftraggebers werden in Einklang mit den Vorgaben des Auftraggebers von den Daten anderer Auftraggeber separiert. Mitarbeiter werden schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Systeme oder Applikationen mit einzubringen oder zu übertragen.

Technische Maßnahmen	Organisatorische Maßnahmen
• DLP-Nutzung. • Einsatz von Multi-User fähigen Applikationen und Systemen zur logischen Trennung der Kundendaten. • Einsatz einer MDM-Lösung für mobile Geräte. • Härtung gemeinsam genutzter VDI oder Applikationsinstanzen. • On-Access-Scan aller eingehenden Daten. • Physische Trennung der Entwicklungs-, Test-, Produktionssysteme. • Trennung zwischen Systembereichen, Datenbanken, Speicher, Betriebssystemen sowie Datennetzen.	• Definition entsprechender Datenbankfelder. • Festlegung von Datenbankrechten. • Protokollierung erfolgt über das jeweilige Berechtigungskonzept der Systeme.

2 Vertraulichkeit, Integrität und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO)

2.6 Maßnahmen zur Weitergabekontrolle

Über die Weitergabekontrolle soll die Sicherheit personenbezogener Daten während der Übertragung und des Transports gewährleistet werden, um unbefugten Zugriff, Kenntnisnahme, Veränderung oder Löschung der Daten zu verhindern. Sie umfasst die Festlegung klarer Regeln für die Weitergabe, die Identifizierung und Überprüfung von Empfängern und die Auswahl sowie Sicherung geeigneter Übertragungswege.

Technische Maßnahmen	Organisatorische Maßnahmen
• Austausch erfolgt nur über geprüfte und freigegebene Protokolle oder Systeme. • Deaktivierung von USB-Schnittstellen. • Einsatz von Gateway- und Firewall-Rechnern gem. Firewall-Policy. • Remote Work nur mittels VPN. • Transportsicherung mittels sicherer Fahrzeuge, Behälter, verschlüsselter Speichermedien inkl. Protokollierung. • Webproxies für alle HTTPS-Verbindungen.	• DLP-Nutzung zur Beschränkung und Kontrolle von Übermittlungen. • Klassifizierung der Datenträger nach Schutzbedarf. • Protokollierung des Datenträgertransports (z. B. Datenträgerabgabe und –empfang; Versand- und Empfangsbestätigungen im Vier-Augen-Prinzip). • Richtlinien für die Durchführung der Transfers. • Verzeichnis über Datenempfänger.

2.7 Maßnahmen zur Belastbarkeit

Über die Maßnahmen zur Belastbarkeit stellt Deloitte die Fähigkeit seiner IT-Systemen und Dienste sicher, auch unter Störungen, Fehlern oder hoher Beanspruchung funktionsfähig zu bleiben, um eine sichere Verarbeitung personenbezogener Daten kontinuierlich zu gewährleisten.

Technische Maßnahmen	Organisatorische Maßnahmen
• Aktiv-Aktiv Rechenzentren für alle Systeme und Anwendungen, • Aktuelle Viren- und Malware Signaturen, • Firewall Systeme, • IDS / IPS Systeme, • Kapazitätsmanagement, • Loadbalancer, • Raid Systeme, • Redundant ausgelegte IT-Systeme, • Regelmäßige Penetration Tests aller Systeme, • Staging Systeme (Dev/QA/Prod), • USV-Systeme	• Arbeitsanweisungen zur Vertretungsregelungen der Mitarbeiter, • Festlegung von Aufbewahrungsfristen, • Content-Security-Policy (CSP), • Logging und Monitoring, • Interne Notfall- und Krisenorganisation, • Organisatorische und technische Regelungen, Arbeitsrichtlinien etc. sind vorhanden und kommuniziert. Diese werden regelmäßig überprüft, • Patch Management Prozess, • Prüfungs- und Wartungsverträge mit Dienstleistern

3 Verfügbarkeit und Wiederherstellung der Systeme und Dienste (Art. 32 Abs. 1 lit. c DSGVO)

3.1 Maßnahmen zur Verfügbarkeit (Sicherung)

Ziel ist es, mithilfe geeigneter Maßnahmen sicherzustellen, dass geschützte Daten nicht verloren gehen oder versehentlich zerstört werden und sie während der geregelten Nutzungszeit stets verfügbar sind.

Technische Maßnahmen	Organisatorische Maßnahmen
• Aktuelle Programmversionen/-patche für Betriebssysteme und Applikationen, • Aktueller Viren-, und Malwareschutz, • Daten-/Programmsicherungen, • Redundante Systeme oder Rechenzentren, • Logging und Monitoring, • Unterbrechungsfreie Stromversorgung	• IT Service Continuity Management, • Durchführung regelmäßiger Übungen zur Wiederherstellung von Daten, • Festlegung der Aufbewahrungsfristen, • Organisatorische und technische Regelungen, Arbeitsrichtlinien etc. sind vorhanden und kommuniziert, • Regelmäßige Prüfung der Richtlinien

3.2 Maßnahmen zur Löschung

Mit den Maßnahmen zur Löschung der Daten nach DSGVO werden diese unwiederbringlich gelöscht bzw. vernichtet, sodass diese nicht mehr auffindbar, nutzbar oder einzelnen Personen zuzuordnen sind. Dies kann durch das Überschreiben elektronischer Daten, die physische Zerstörung von Datenträgern oder durch Anonymisierung erreicht werden.

Technische Maßnahmen	Organisatorische Maßnahmen
• Akten, Papier, Dokumente – Aktenvernichter / Schredder (mind. Stufe P4), – Schreddern vor-Ort im LKW unter Aufsicht, – Verschlossene Papiertonnen vor-Ort • Löschung oder Vernichtung nach DIN 66399 elektronischer Daten oder Speichermedien mindestens nach Stufe 4 – Mehrfaches Überschreiben (7-fach), – Schreddern (mind. Stufe E4 / H4) bei streng vertraulichen Daten immer oder wenn Löschen/Überschreiben fehlschlägt	• Protokollierung der Löschung von Daten aufgrund gesetzlicher Erfordernisse. • Richtliniendokument zu Aufbewahrungs-, und Löschfristen. • Verfahren zur Löschung von elektronischen Daten und Speichermedien. • Verfahren zur Vernichtung von Akten und Papieren.

3 Verfügbarkeit und Wiederherstellung der Systeme und Dienste (Art. 32 Abs. 1 lit. c DSGVO)

3.3 Recovery measures

The aim of recovery measures is to quickly restore data availability in the event of a malfunction and to prevent data loss due to destruction or unauthorized alteration of data.

Technische Maßnahmen	Organisatorische Maßnahmen
• Durchführung mindestens einer Krisenstabsübung pro Jahr samt Dokumentation. • Durchführung von Notfallübungen samt Dokumentationen. • Durchführung von Schulungen des Krisenstabs, der Krisenorganisation sowie der Mitarbeiter.	• Eine Krisenorganisation samt Krisenstab ist vorhanden. • Notfallpläne (DRP) sind dokumentiert und werden regelmäßig aktualisiert. • Deloitte ist nach ISO 22301 zertifiziert.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs (PDCA-Zyklus)
(Art. 25 Abs. 1 DSGVO)

4.1 Maßnahmen zur Auftragskontrolle (Art. 28, 25 Abs. 1 DSGVO)

Ziel der Auftragskontrolle ist, dass personenbezogene Daten, die im Auftrag verarbeitet werden, entsprechend den vorgegebenen Weisungen verarbeitet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
	• Durchführung von Datenschutz-Folgenabschätzungen, soweit gesetzlich erforderlich. • Eindeutige und umfassende vertragliche Regelungen für alle Auftragsarbeiten. • Einhaltung der relevanten DSGVO-Vorschriften. • Kriterien zur Auswahl von Unterauftragnehmern. • Vorgaben für Rahmen- und Einzelaufträge. • Für Unterauftragnehmer, von denen Daten erhoben bzw. an die Daten übermittelt werden: – Existiert ein Prozess zur Prüfung und Dokumentation – Ist eine risikobasierte Regelüberprüfung über durch aktuelle Zertifizierung, Audits oder Self-Assessments erforderlich – Verfügen über adäquate TOMs und Zertifizierungen, basierend auf dem zugrunde liegenden Schutzniveau – Verfügen über eindeutige vertragliche Regelungen.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs (PDCA-Zyklus)
(Art. 25 Abs. 1 DSGVO)

4.2 Maßnahmen zur Ausführung / Umsetzung

Ziel der regelmäßigen Überprüfungen ist es, einen kontinuierlichen Verbesserungsprozess zu leben, der den Umgang mit personenbezogenen Daten optimiert und sich an die vertraglichen und regulatorischen Anforderungen anpasst.

Technische Maßnahmen	Organisatorische Maßnahmen
• Einsatz eines Tools zur Dokumentation und Auswertung von Sicherheitsvorfällen.	• Ein (Security) Incident Management nach DSGVO existiert zur – fristgerechten Meldung an Behörden und Kunden, – Angriffserkennung (Incident-Response), – forensischen Analyse von Sicherheitsvorfällen. • Ein Informationsmanagementsystem ist nach ISO 27001 implementiert und zertifiziert. • Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO. • Regelmäßige Überprüfung der TOMs. • Regelmäßige Überprüfung der Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden. • Rollen und Verantwortlichkeiten im Bereich Datenschutz und Informationssicherheit sind definiert, besetzt und intern bekannt. • Sicherheitsrichtlinien für den Umgang mit Informationen sind definiert und durch das Management kommuniziert. • Sicherstellung der Einhaltung der relevanten DSGVO-Vorschriften. • Zur Sicherung der Auftragsdurchführung werden interne und externe Überprüfungen der internen Abläufe und externen Dienstleister durchgeführt, im Rahmen der ISO 9001, ISO 22301 und ISO 27001 Zertifizierungen von Deloitte.

5 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

5.1 Maßnahmen für datenschutzfreundliche Voreinstellungen

Der Schutz der Privatsphäre und die Durchsetzung von Datenschutzgrundsätzen von Beginn an sind die Ziele einer „*Datenschutz durch Technikgestaltung*“ bzw. „*Privacy by Design*“. Durch geeignete Voreinstellung stellt Deloitte sicher, dass personenbezogene Daten mit dem größtmöglichen Datenschutz verarbeitet werden, damit diese Daten von vornherein nicht einer unbestimmten Zahl von Personen zugänglich gemacht werden. Diese „*datenschutzfreundlichen Voreinstellungen*“ bzw. „*Privacy by Default*“ bekannt. Ein weiteres Ziel von „*Privacy by Default*“ ist es, auch solchen Betroffenen, die keine oder wenig Kenntnisse zu Datenschutzeinstellungen haben, ein Mindestmaß an Datenschutz zu ermöglichen.

Technische Maßnahmen	Organisatorische Maßnahmen
	• Konzept zur Identifizierung der Datenflüsse von personenbezogenen Daten und der involvierten IT-Komponenten. • Konzept zur Sicherstellung von Löschfristen, Datenminimierung und Zugriffbeschränkungen im Rahmen von Software-Beschaffungsprozessen, -Entwicklungsprozessen und -Änderungsprozessen. • Konzept zur Umsetzung von Löschfristen, Datenminimierung und Zugriffsbeschränkungen im Rahmen der System- und Applikationskonfiguration.

Deloitte.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter http://www.deloitte.com/de/UeberUns.

Deloitte bietet führende Prüfungs- und Beratungsleistungen für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeitenden liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, und unsere Kunden bei Wandel und Wachstum unterstützen. Deloitte baut auf eine 180-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 470.000 Mitarbeitenden von Deloitte das Leitbild „making an impact that matters“ täglich leben: www.deloitte.com/de.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen, und weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeitende oder Bevollmächtigte haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbständige und unabhängige Unternehmen.