Richtlinie Informationssicherheit und Datenschutz für Lieferanten

Inhalt

1 Einführung und Geltungsbereich

1.1 Einleitung

In dieser Richtlinie werden Regeln für den Umgang mit Informationen und den Einsatz von Informationstechnik definiert, die Lieferanten und Dienstleister (Auftragnehmer) der Montaplast GmbH zu befolgen haben. Zweck dieser Richtlinie ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Rechte und Interessen des Auftraggebers sowie aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit dem Auftraggeber eingehen und / oder Tätigkeiten für diesen ausführen.

1.2 Geltungsbereich

Diese Richtlinie richtet sich an die Geschäftsleitung des Lieferanten / Dienstleisters, deren Mitarbeiter sowie deren Erfüllungs- /Verrichtungsgehilfen.

Dienstleister sind definiert als Dritte, die Leistungen für die Montaplast GmbH auf Basis vertraglicher Beziehungen erbringen.

2 Wahrung von Vertraulichkeit von Informationen/Betriebsgeheimnissen

(1) Der Auftragnehmer und seine Subunternehmen sind verpflichtet, die vom Auftraggeber eingeräumten Zugangs-/Zugriffsrechte (IT-Systeme, Dienste, Daten und Anwendungen) ausschließlich im Rahmen ihrer vertraglich zu erfüllenden Verpflichtungen zu nutzen.

(2) Sämtliche durch den Auftrag erlangte, nicht öffentlich bekannte Informationen sowie auftragsbedingt erstellte Kopien, Aufzeichnungen und Arbeitsergebnisse sind Eigentum des Auftraggebers und an diesen nach Beendigung des Auftrages heraus-bzw. zurückzugeben.

(3) Der Auftragnehmer und seine Subunternehmen sind verpflichtet, alle ihm im Zusammenhang mit der Vertragserfüllung zur Kenntnis gelangten Informationen über den Arbeitgeber,

(4) ihre Geschäfts- und Betriebsangelegenheiten und alle Arbeitsergebnisse vertraulich zu behandeln und angemessen gegen eine Kenntnisnahme durch Unberechtigte und nicht vertragsgemäße Nutzung, Vervielfältigung oder Weitergabe zu schützen. Die Verpflichtungen gelten über die Beendigung des Vertragsverhältnisses hinaus. Dem Auftragnehmer ist nicht gestattet, sich geschäftliche oder betriebliche nicht öffentlich bekannt gemachte Informationen gleich welcher Art über Auftraggeber und/oder seine Kunden, Lieferanten oder Mitarbeiter anzuzeigen, für eigene Zwecke zu nutzen oder Kopien oder Aufzeichnungen irgendwelcher Art zu fertigen, soweit dies nicht zur Erfüllung des Auftrags erforderlich ist. Solche Informationen, Kopien, Aufzeichnungen oder Arbeitsergebnisse dürfen nicht an Dritte weitergegeben oder Dritten zur Kenntnis gebracht werden.

(5) Vertrauliche Informationen dürfen nur an die Subunternehmen weitergegeben werden, für die der Auftraggeber seine Zustimmung erteilt hat und die auf die Einhaltung der vorliegenden Sicherheitsrichtlinien verpflichtet wurden.

(6) Der Auftragnehmer darf beim Auftraggeber nur auf das Datengeheimnis, die Informationssicherheit und ggf. auf sonstige Geheimnisse verpflichtetes Personal einsetzen. Die Verpflichtungen bestehen auch nach Beendigung der Tätigkeit fort.

3 Formen der Zusammenarbeit

Der Einsatz von externen Partnern zeichnet sich primär dadurch aus, dass für die Unterstützung von Arbeits- oder Geschäftsprozessen sowie des Betriebs von Anwendungen und Systemen des Unternehmens externe Personen vertraglich beauftragt werden.

Motivationen gibt es viele, externen Partnern den Zugriff auf Unternehmensdaten oder Unternehmens-Systeme zu geben. Manche Firmen benötigen z.B. den Zugriff zu Wartungs-, Service- oder Testzwecken, andere Firmen müssen Systeme im Auftrag des Unternehmens "bedienen". Ebenso können komplette Services z.B. im Rahmen von Outsourcing oder Cloud Computing an externe Partner vergeben werden.

Prinzipiell ist mit jedem Fremdfirmenzugriff auf Montaplast Unternehmensdaten oder der ausgelagerten Verarbeitung von Daten auch ein potenzielles Risiko missbräuchlicher Nutzung verbunden. Es besteht z.B. das Risiko, dass die mit einem Fremdfirmenzugang verbundenen Zugriffsrechte dazu verwendet werden, das Umfeld im Unternehmens-Netz zu erkunden und auf andere Systeme als die explizit freigegebenen zuzugreifen oder dass Informationen aus Anwendungssystemen beschafft werden, die nicht direkt mit dem Auftrag des Unternehmens zu tun haben.

Informationen, die verarbeitet werden bzw. auf die zugegriffen wird, sind hierbei wesentliche Vermögenswerte der Montaplast GmbH. Das Informationssicherheit-Managementsystem der Montaplast GmbH sieht Sicherheitsmaßnahmen zur Gewährleistung eines Grundschutzes für Daten, Informationen und die zugrundeliegende Infrastruktur vor. Zur Erreichung eines durchgängigen Grundschutzes ist es erforderlich, die Sicherheitsstandards auch im Rahmen der Zusammenarbeit mit externen Auftragnehmern anzuwenden. Je nach Art der Zusammenarbeit können sich unterschiedliche Anforderungen an die umzusetzenden Sicherheitsmaßnahmen ergeben. Grundsätzlich gelten die definierten Sicherheitsregelungen für alle internen und externen Mitarbeiter.

Im Bereich der Zusammenarbeit mit externen Partnern sind verschiedene Formen der Zusammenarbeit möglich. Für die Anwendung der Montaplast Sicherheitsvorgaben wurden unterschiedliche Typen der Zusammenarbeit definiert.

Formen der Zusammenarbeit	
Typ	**Beschreibung der Zusammenarbeit mit dem externen Partner**
Typ 1: Externe Datenbearbeitung (ohne Netzanbindung und Remote-Zugriff)	Es werden Daten des Auftraggebers auf den Systemen des Auftragnehmers gehalten. Der Auftragnehmer bekommt beispielsweise im Rahmen eines Design-, Entwicklungs- oder Konstruktionsauftrages die Daten des Auftraggebers übermittelt oder wird etwa als Softwareentwickler für den Auftraggeber tätig. Er verarbeitet die Daten selbstständig auf eigenen Systemen. Der Auftragnehmer erhält die Daten vom Auftraggeber via Datenträger (USB-Medien, Tapes, etc.), E-Mail oder auf andere Weise im Rahmen eines Informationsaustausches (VDA-/Odette-DFÜ-Kommunikation, File-Transfer, Download etc.).
Typ 2: Datenverarbeitung auf Systemen des Auftragnehmers (Outsourcing, Cloud, Netzkopplung, etc.)	Der Auftragnehmer nimmt etwa im Auftrag des Auftraggebers die Informationsverarbeitung auf eigener Hard- und Systemsoftware vor. Der Auftragnehmer stellt hierbei beispielsweise die Betriebssysteme, Anwendungssysteme und/oder Kommunikationskomponenten zur Verfügung. Der Auftraggeber ist verantwortlich für die Daten, wobei es sich bei der Verarbeitung der Daten um schutzbedürftige (personenbezogene) Informationen / Daten handelt. Im Fall der Verarbeitung personenbezogener Daten liegt eine Auftragsverarbeitung vor. Neben der Anbindung des Auftragnehmers auf Basis von Routern/Firewalls, Modem/Kommunikationsservern sowie des Internets, kommt auch die

Formen der Zusammenarbeit	
Typ	**Beschreibung der Zusammenarbeit mit dem externen Partner**
	Direkteinbindung des Auftragnehmers in die IT Infrastrukturen des Auftraggebers in Frage, z.B. Cloud Computing, SasS etc. – Der Auftragnehmer greift auf Systeme des Auftraggebers zu. – Es werden Daten des Auftraggebers auf den Systemen des Auftragnehmers gehalten. – Der Auftraggeber übermittelt Daten an den Auftragnehmer, dieser bearbeitet die Daten auf seinen Systemen.
Typ 3: Vor-Ort-Zugriff	Der Auftragnehmer greift am Standort des Auftraggebers auf Daten zu und übernimmt die Funktion des Benutzerservices (Second-Level-Support) für die Endanwender (Beratung, Problemhilfe, Fehlerbehebung). Als Betreiber übernimmt der Auftragnehmer die Betriebsverantwortung von Netzen, Systemen und Applikationen. Als Softwareentwickler hat der Auftragnehmer Zugriff auf die IV-Infrastruktur. Der Auftragnehmer ist im Falle des Vor-Ort-Zugriffes i.d.R. direkt in die IT-Infrastrukturen des Auftragnehmers eingebunden. Es werden keine personenbezogenen Daten bzw. schutzbedürftige Informationen auf den Systemen des Auftragnehmers verarbeitet.
Typ 4: Remote-Zugriff bzw. Direktkopplung	Beim Remote-Zugriff sind zwei Fälle zu unterscheiden: 1. Es besteht ein Remote-Zugriff des Auftragnehmers auf die Systeme und Applikationen des Auftraggebers über eine Netzverbindung. Anwendungsbeispiele: – Der Auftragnehmer wird als Client in eine Client/Server-Anwendung des Auftraggebers direkt in den Arbeitsprozess eingebunden. – Der Auftragnehmer ist Teilnehmer an einer WEB-Konferenz, einem Online Meeting, etc. – Der Auftragnehmer nimmt an den vielfältigen Formen der Bürokommunikation teil. – Der Auftragnehmer führt Fernwartungen an IT-Systemen oder Anlagen des Auftraggebers oder sonstigen netzintegrierten Systemen durch. 2. Es bestehen Remote-Zugriffe von Subunternehmern, Telearbeitern, etc. auf Systeme und Applikationen beim Auftragnehmer. Die Anbindung erfolgt auf Basis von Router/Firewall, Internet- oder VPN-Verbindungen bzw. ISDN/Modem/Kommunikationsserver. Es werden keine personenbezogenen Daten bzw. schutzbedürftige Informationen auf den Systemen des Auftragnehmers verarbeitet.
Typ 5: System-Überlassung durch den Auftraggeber	Der Auftraggeber stellt dem Auftragnehmer ein System zur Nutzung zur Verfügung, mit dem der Auftragnehmer in die Infrastruktur des Auftraggebers integriert werden kann. Die Sicherheitskonfigurationen und Standards werden vom Auftraggeber festgelegt. (Beispiel: Mitarbeiter des Auftragnehmers arbeiten mit vom Auftraggeber gestellten Systemen in den Räumen des Auftraggebers oder bekommen Geräte zur Nutzung überlassen.)
Typ 6: Physische Objekte /Informationen	Es werden physisch schützenswerte Informationen wie beispielsweise Ordner, Konzepte, Verträge, Muster, Prototypen, Komponenten, Werkzeuge, Vorrichtungen, etc. sowie begleitende Informationen und Daten beim Auftragnehmer bearbeitet, erstellt oder gelagert, die vom Auftraggeber als „vertraulich" oder „geheim" klassifiziert wurden.
Hinweis: Mischformen werden die Regel sein	

4 Anforderungen an Auftragnehmer zur Aufrechterhaltung der Informationssicherheit

4.1 Grundsätzliches

Im Rahmen der Zusammenarbeit sind grundsätzlich die Vorgaben des Informationssicherheits-und Datenschutz-Managementsystems der Montaplast GmbH einzuhalten. Die Auftragnehmer sind grundsätzlich verpflichtet, sich beim Auftraggeber über die aktuell gültigen Richtlinien vor Aufnahme der Tätigkeit zu informieren. Zur Einhaltung der Anforderungen der Datenschutzgrundverordnung (DSGVO) kann es erforderlich sein, je nach Art und Umfang der verarbeiteten Daten Verträge zur Auftragsverarbeitung (Art. 28 DSGVO) oder zur gemeinsamen Verantwortung (Art. 26 DSGVO) abzuschließen. Dies ist im Einzelfall mit dem Auftraggeber abzustimmen.

Der Auftragnehmer wird aufgefordert ein Informationssicherheits-Managementsystem gemäß den Anforderungen der ISO 27001/27002 umzusetzen und die gesetzlichen Anforderungen zum Datenschutz einzuhalten.

In Abhängigkeit der Form der Zusammenarbeit ergeben sich Schwerpunkte bei den Anforderungen der umzusetzenden Maßnahmen. Diese sind im Kapitel 7 dargestellt. Im Laufe der Geschäftsbeziehung kann sich die Form der Zusammenarbeit ändern. In diesem Zusammenhang ändern sich auch die umzusetzenden Sicherheitsmaßnahmen. Im Folgenden sind die Anforderungen an das Informationssicherheits-Managementsystem des Auftragnehmers dargestellt.

4.2 Organisation der Informationssicherheit

Es sind Richtlinien, Prozesse und Verantwortlichkeiten zu definieren, mit denen die Informationssicherheit implementiert und kontrolliert werden kann.

Dies beinhaltet insbesondere:

- Die Erstellung einer Informationssicherheitsrichtlinie.
- Anwenderrichtlinien zur Festlegung von Regeln für den Umgang mit Anwendungen, Systemen und IT-Endgeräten und dem Verhalten bei der Nutzung von Informationstechnologie.
- Die Beschreibung von Prozessen für die Verwaltung von Datenträgern, Dokumenten und Informationen.
- Die Festlegung der Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit.
- Die Verpflichtung der Mitarbeiter auf Geheimhaltung und Wahrung des Datengeheimnisses.
- Die regelmäßige Durchführung von Schulungen und Awareness-Maßnahmen.

4.3 Privacy by Design (nur relevant bei personenbezogenen Daten)

Privacy by Design beinhaltet den Gedanken, dass Systeme so konzipiert und beschaffen sein sollten, dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird. Wesentliche Elemente der Datensparsamkeit sind die Trennung personenbezogener Identifizierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und die Anonymisierung. Außerdem muss das Löschen von personenbezogenen Daten gemäß einer konfigurierbaren Aufbewahrungsfrist realisiert sein.

Dies beinhaltet insbesondere:

- Es werden nicht mehr personenbezoenene Daten erhoben als für den Zweck erforderlich sind.
- DSGVO konformes Löschen der verarbeiteten personenbezogenen Daten ist sichergestellt.
- Bei Änderung und Einführung von Systemen und Anwendungen wird Privacy by Design berücksichtigt.

4.4 Privacy by Default (nur relevant bei personenbezogenen Daten)

Die Systeme und Anwendungen müssen so eingestellt werden, dass datenschutzfreundlichen Voreinstellungen/Standardeinstellungen vorliegen und möglichst wenig personenbezogene Daten erfasst werden.

Dies beinhaltet insbesondere:

- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen.
- Trackingfunktionen, die den Betroffenen überwachen, sind standardmäßig deaktiviert.
- Sämtliche Vorbelegungen von Auswahlmöglichkeiten erfüllen die Anforderungen der DSGVO in Bezug auf datenschutzfreundliche Voreinstellungen (z.B. keine Vorbelegungen von Opt-ins).

4.5 Zugriffskontrolle

Umsetzung von Maßnahmen, die gewährleisten, dass die zur Benutzung der Informationsverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten bzw. schutzbedürftigen Informationen und Daten zugreifen können

Dies beinhaltet insbesondere:

- Die Erstellung von Berechtigungskonzepten für den Zugriff auf schützenswerte Informationen, Systeme und Applikationen.
- Die Umsetzung von Zugriffsbeschränkungen.
- Die Vermeidung der Konzentration von Funktionen und Etablieren einer Funktionstrennung.
- Die Umsetzung eines Prozesses zur Berechtigungsvergabe.
- Die regelmäßige Überprüfung der Berechtigungen.
- Die Protokollierung der Berechtigungsvergabe und des Datenzugriffs.

4.6 Kryptographie und / oder Pseudonymisierung

Der Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes der Vertraulichkeit, Authentizität oder Integrität von personenbezogenen Daten bzw. schutzbedürftigen Informationen. Maßnahmen bei der Verarbeitung von personenbezogenen Daten, die geeignet sind, eine Identifikation des Betroffenen zu erschweren.

Dies beinhaltet insbesondere:

- Die Verschlüsselung von Datenträgern und Festplatten von PC, Laptops, mobilen Endgeräten und Verzeichnissen.
- Die gesicherte Speicherung von Daten auf mobilen Datenträgern. Als vertrauliche oder geheim klassifizierte Daten sind auf mobilen Datenträgern zu verschlüsseln.
- Organisatorische Anweisung für die Verschlüsselung von Daten.
- Verschlüsselte Ablage von personenbezogenen Daten.
- Verschlüsselung von Datensicherungsmedien (z.B. Bänder, Festplatten etc.).
- Verschlüsselung von Zugängen zum Netzwerkzugängen und -verbindungen.
- Einsatz von Pseudonymen, Verfahren zur Pseudonymisierung von Daten.
- Einsatz Verfahren zur Anonymisierung von Daten.

4.7 Schutz von Gebäuden

Umsetzung von Maßnahmen, die den unautorisierten physischen Zugriff auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung verhindern.

Dies beinhaltet insbesondere:

- Die Festlegung von Sicherheitsbereichen.
- Die Realisierung des Zutrittsschutzes.
- Die Festlegung zutrittsberechtigter Personen.
- Die Verwaltung von personengebundenen Zutrittsberechtigungen.
- Die Regelungen zur Begleitung von Besuchern und Fremdpersonal.
- Die Überwachung der Räume außerhalb der Schließzeiten.
- Die Protokollierung des Zutritts.

4.8 Schutz von Betriebsmitteln / Informationswerten

Es sind geeignete Schutzmaßnahmen zur Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Betriebsmitteln / Informationswerten und zur Vermeidung von Unterbrechungen der Betriebstätigkeit der Organisation zu implementieren.

Dies beinhaltet insbesondere:

- Regelungen zur sicheren Platzierung von Betriebsmitteln.
- Schutz der Betriebsmittel vor Überspannung, Stromausfall, Wasser und Feuer.
- Schutz vor Diebstahl.
- Regelungen zur regelmäßigen Wartung von Betriebsmitteln.
- Die Implementierung eines Prozesses zur sicheren Löschung, Entsorgung und Vernichtung von Betriebsmitteln.

4.9 Betriebsverfahren und Zuständigkeiten

Es ist der ordnungsgemäße und sichere Betrieb von Systemen und Verfahren zur Verarbeitung von Informationen sicherzustellen.

Dies beinhaltet insbesondere:

- Die Dokumentation der Betriebsverfahren.
- Die Härtung der Backend Systeme.
- Die getrennte Verarbeitung von Produktiv- und Testdaten.
- Sicherstellung der Mandantentrennung / Mandantenfähigkeit.
- Die Anforderungen einer Funktionstrennung sind umzusetzen. Es ist festzulegen, zu dokumentieren und zu begründen, welche Funktionen nicht miteinander vereinbar sind, also nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Grundsätzlich sind dabei operative Funktionen nicht mit kontrollierenden Funktionen vereinbar.

4.10 Datensicherungen

Es sind Maßnahmen umzusetzen, die gewährleisten, dass schutzbedürftige Informationen und Daten / personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Dies beinhaltet insbesondere:

- Die Erstellung eines Datensicherungskonzeptes.
- Es sollten regelmäßige Datensicherungen durchgeführt werden.
- Die Datensicherungsmedien sind getrennt aufzubewahren.

4.11 Schutz vor Malware durch Schwachstellen-und Patchmanagement

Eine Ausnutzung technischer Schwachstellen sind durch den Einsatz von aktueller Virenschutzsoftware und die Implementierung eines Patchmanagements zu verhindern. Es wird empfohlen, regelmäßige Überprüfungen zur Erkennung von Schwachstellen durchzuführen.

Dies beinhaltet insbesondere:

- Regelmäßige Überwachung des Status von Sicherheitsupdates und Systemschwachstellen.
- Einsatz von Anti-Malware-Software.
- Regelmäßiges Einspielen von Sicherheitspatches und Updates.

4.12 Protokollierung und Überwachung

Es sind Maßnahmen zu implementieren, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem (personenbezogene) Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind. (Sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens 3 Jahre lang durch den Auftragnehmer aufbewahrt.)

Dies beinhaltet insbesondere:

- Die Protokollierung der Berechtigungsvergabe und des Datenzugriffs.
- Die Überprüfung von Benutzerberechtigungen.
- Die Protokollierung der Aktivitäten und regelmäßige Auswertung der Benutzer- und Systemaktivitäten.

4.13 Netzwerksicherheitsmanagement

Es muss ein angemessener Schutz für das Netzwerk implementiert werden, so dass die Informationen und die Infrastrukturkomponenten geschützt werden.

Dies beinhaltet insbesondere:

- Die Implementierung eines Netzwerkmanagements.
- Die Umsetzung einer Benutzerauthentifizierung für externe Verbindungen und Verbindungen zwischen einzelnen Systemen.
- Die Gewährleistung eines Schutzes der Diagnose- und Konfigurationsports.
- Sicherheitsgateways an den Übergabepunkten / Netzgrenzen.
- Die Isolation sensitiver Systeme.

4.14 Informationsübertragung

Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten bzw. schutzbedürftiger Informationen und Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

(Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)

Dies beinhaltet insbesondere:

- Den sicheren Transport und den Versand von Daten / Dokumenten in Abhängigkeit vom Schutzbedarf der Daten.
- Die Protokollierung der Datenübertragungen.
- Die Beschreibung von Schnittstellen zwischen Systemen und der externen Datenverbindungen.
- Angemessener Schutz von Emails, die sensible Informationen / Daten beinhalten.
- Den Abschluss von Verträgen zum Schutz von Geschäftsgeheimnissen mit Dritten und Unterlieferanten.

4.15 Netztrennung

Gruppen von Informationsdiensten, Mandanten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden.

Dies beinhaltet insbesondere:

- Gruppen von Informationsdiensten, Mandanten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden.
- Um das Risiko zu mindern, dass personenbezogene Daten bzw. schutzbedürftige Informa-tionen und Daten, die zwischen IT-Systemen weitergegeben werden, auf dem Netz mitge-lesen werden, sind diese zu segmentieren.
- Direkte Verbindungen des Clients zum Internet sind bei remote Zugriffen (z.B. über VPN oder RAS) auf das Unternehmensnetz durch geeignete Maßnahmen zu unterbinden.

4.16 Anschaffung, Entwicklung und Instandhaltung von Systemen

Maßnahmen, die sicherstellen, dass Informationssicherheit ein fester Bestandteil über den Lebenszyklus von Informationssystemen ist.

Dies beinhaltet insbesondere:

- Die Festlegung von sicherheitsspezifischen Regelungen und Anforderungen für den Einsatz neuer Informationssysteme und für die Erweiterung bestehender Informationssysteme.
- Die Festlegung von Regelungen für die Entwicklung und Anpassung von Software und Systemen.
- Entwicklung von Leitlinien zur sicheren Systementwicklung.
- Die Überwachung von ausgelagerten Systementwicklungstätigkeiten.
- Den Schutz von Testdaten.

4.17 Lieferantenbeziehungen bzw. Auftragsverarbeitung

Maßnahmen an die Informationssicherheit, zur Verringerung von Risiken, im Zusammenhang mit dem Zugriff von Lieferanten auf die Werte des Unternehmens, sollten mit Sublieferanten / Subunternehmern vereinbart und dokumentiert werden.

Dies beinhaltet insbesondere:

- Die schriftliche Adressierung von Sicherheitsthemen in Verträgen mit Sublieferanten.
- Die Überprüfung der Sicherheit bei Subunternehmern.
- Die Festlegung von technisch organisatorischen Maßnahmen (TOMs) bei Verarbeitung personenbezogener Daten.

- Die laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten.

4.18 Management von Informationssicherheitsvorfällen

Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall, Datenverlust etc.) zu implementieren.

Dies beinhaltet insbesondere:

- Die unverzügliche Meldung von Informationssicherheitsvorfällen an den Auftraggeber.
- Die Protokollierung von Sicherheitsvorfällen.
- Die Implementierung von Prozessen zur Behandlung und Vermeidung von Informationssicherheitsvorfällen.

4.19 Informationssicherheitsaspekte des Business Continuity Management / Notfallmanagements

Die Aufrechterhaltung der Systemverfügbarkeit in schwierigen Situationen wie Krisen- oder Schadensfällen muss aufrechterhalten werden. Ein Notfallmanagement muss dieses sicherstellen. Die Anforderungen bezüglich der Informationssicherheit sollten bei den Planungen zur Betriebskontinuität und Notfallwiederherstellung festgelegt werden.

Dies beinhaltet insbesondere:

- Die Schaffung von Redundanzen.
- Risikoabschätzung und Planung von Maßnahmen zur Sicherstellung des Geschäftsbetriebes.
- Erstellung von Notfallplänen.
- Regelmäßige Tests bzgl. der Wirksamkeit der Notfallmaßnahmen.
- Frühzeitige Information des Auftraggebers bei Notfällen.

4.20 Einhaltung gesetzlicher und vertraglicher Anforderungen

Implementierung von Maßnahmen zur Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen sowie gegen jegliche Sicherheitsanforderungen.

Dies beinhaltet insbesondere:

- Geheimhaltungsverpflichtungen mit Mitarbeitern sowie Sublieferanten.
- Sicherstellung der Einhaltung der gesetzlichen Verpflichtungen im Rahmen der Zusammenarbeit.
- Rückgabe sämtlicher Daten, Betriebsmittel und Informationswerte an den Auftraggeber bei Vertragsende.

4.21 Datenschutzanforderungen und Datenschutzmanagement (nur relevant bei personenbezogenen Daten)

Die Privatsphäre sowie der Schutz von personenbezogenen Daten sollten entsprechend den Anforderungen der relevanten Gesetze, Vorschriften und ggf. Vertragsbestimmungen sichergestellt werden.

Dies beinhaltet insbesondere:

- Die Bestellung eines Datenschutzbeauftragten wenn gesetzlich erforderlich.
- Den Aufbau eines Datenschutzmanagements.
- Die Erstellung von Verfahrensverzeichnissen.

- Den Aufbau eines Datenschutznotfall Managements.
- Die Durchführung regelmäßiger Überprüfungen / Audits zur Bestimmung des Datenschutzniveaus.
- Die Einhaltung der gesetzlichen Anforderungen im Rahmen der Auftragsdatenverarbeitung.

4.22 Informationssicherheitsüberprüfungen

Es muss regelmäßig überprüft werden, ob die Informationsverarbeitung entsprechend der definierten Sicherheitsmaßnahmen durchgeführt wird. Hierfür wird der Auftragnehmer regelmäßige Prüfungen durchführen. Der Auftragnehmer räumt dem Auftraggeber das Recht ein, regelmäßige Prüfungen beim Auftragnehmer durchzuführen.

5 Informationspflichten des Auftragnehmers

Der externe Partner muss den Auftraggeber unverzüglich über Informationssicherheitsvorfälle, bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers; insbesondere solche Vorfälle, die einen Zugriff durch Unbefugte möglich machen., informieren.

Sollten die Daten des Auftraggebers beim externen Partner durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

Die Meldungen sind an die zentrale E-Mail Adresse: ISMS-Beauftragter@montaplast.com zu richten.

6 Überprüfung der Umsetzung von Sicherheitsmaßnahmen

Montaplast behält sich das Recht vor die Umsetzung der in Kapitel 4 dargestellten Sicherheits-Anforderungen zu überprüfen.

Für die Überprüfung kommt die jeweils gültige Version der ISO 27001, des VDA Fragebogens und/oder ein individuelles Assessment zum Einsatz. Alternativ kann die Einhaltung der Informationssicherheit auch über gültiges ISO 27001 Zertifikat, ein TISAX Assessment oder durch eine andere gleichwertige Überprüfung nachgewiesen werden.

7 Anhang Sicherheitsmaßnahmen in Abhängigkeit der Form Zusammenarbeit

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrga verarbeitet werden)			**Formen der Zusammenarbeit**					
Nr	**Referenz ISO 27001/ DSGVO**	**Technisch-organisatorische Maßnahme**	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4. Remote-Zugriff bzw. Direktkopplung	5. System-Überlassung durch den Auftraggeber	6. Physische Objekte /Informationen
01	**A.05** **A.06** **A.07** **A.08**	**Organisation der Informationssicherheit** Festlegungen von Richtlinien, Prozessen und Verantwortlichkeiten mit denen die Informationssicherheit implementiert und kontrolliert werden kann. Allgemeine Anforderungen: - Informationssicherheitsrichtlinie. - Anwenderrichtlinien für den Umgang mit Geräten und dem Verhalten bei der Nutzung von Informationstechnologie. - Prozesse für die Verwaltung von Datenträgern. - Festlegung der Rollen und Verantwortlichkeiten. - Verpflichtung der Mitarbeiter auf Geheimhaltung und Wahrung des Datengeheimnisses. - Regelmäßige Durchführung von Schulungen und Awareness-Maßnahmen.	x	x	x	x		x
02	**A.06** **A.14** **A.18** **Art 25 (1)**	**Privacy by Design** Systeme und Anwendungen sollen so konzipiert und beschaffen sein, dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird. Wesentliche Elemente der Datensparsamkeit sind die Trennung personenbezogener Identifizierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und die Anonymisierung. Außerdem muss das Löschen von personenbezogenen Daten gemäß einer konfigurierbaren Aufbewahrungsfrist realisiert sein. Allgemeine Anforderungen: - Es werden nicht mehr personenbezoenene Daten erhoben als für den Zweck erforderlich sind. - DSGVO konformes Löschen der verarbeiteten personenbezogenen Daten ist sichergestellt. - Bei Änderung und Einführugn von Systemen und Anwendungen wird Privacy by Design berücksichtigt.	AV	AV	AV	AV		AV

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrga verarbeitet werden)			**Formen der Zusammenarbeit**					
Nr	**Referenz ISO 27001/ DSGVO**	**Technisch-organisatorische Maßnahme**	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4. Remote-Zugriff bzw. Direktkopplung	5. System-Überlassung durch den Auftraggeber	6. Physische Objekte /Informationen
03	**A.06** **A.14** **A.18** **Art 25 (2)**	**Privacy by Default** Die Systeme und Anwendungen müssen so eingestellt werden, dass datenschutzfreundlichen Voreinstellungen/Standardeinstellungen vorliegen und möglichst wenig personenbezogene Daten erfasst werden. Allgemeine Anforderungen: - Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen. - Trackingfunktionen, die den Betroffenen überwachen, sind standardmäßig deaktiviert. - Sämtliche Vorbelegungen von Auswahlmöglichkeiten erfüllen die Anforderungen der DSGVO in Bezug auf datenschutzfreundliche Voreinstellungen (z.B. keine Vorbelegungen von Opt-ins).	**AV**	**AV**	**AV**	**AV**		
04	**A.09** **Art 32 (1) b**	**Zugriffskontrolle** Umsetzung von Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten bzw. schutzbedürftigen Informationen und Daten zugreifen können. Allgemeine Anforderungen: - Erstellen eines Berechtigungskonzeptes. - Umsetzungen von Zugriffsbeschränkungen. - Vermeidung der Konzentration von Funktionen und Etablieren einer Funktionstrennung. - Umsetzen eines Prozesses zur Berechtigungsvergabe. - Regelmäßige Überprüfung der Berechtigungen. - Protokollierung der Berechtigungsvergabe und des Datenzugriffs.	**x**	**x**	**x**	**x**		
05	**A.10** **Art 32 (1) a**	**Kryptographie und / oder Pseudonymisierung** Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes der Vertraulichkeit, Authentizität oder Integrität von personenbezogenen Daten bzw. schutzbedürftigen Informationen. Allgemeine Anforderungen: - Verschlüsselung von Datenträgern und Festplatten von PC, Laptops, mobilen Endgeräten und Verzeichnissen. - Gesicherte Speicherung von Daten auf mobilen Datenträgern. - Organisatorische Anweisung für die Verschlüsselung von Daten - Verschlüsselte Ablage von personenbezogenen Daten. - Verschlüsselung von Datensicherungsmedien	**x**	**x**		**x**		

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrga verarbeitet werden)			**Formen der Zusammenarbeit**					
Nr	**Referenz ISO 27001/ DSGVO**	**Technisch-organisatorische Maßnahme**	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4. Remote-Zugriff bzw. Direktkopplung	5. System-Überlassung durch den Auftraggeber	6. Physische Objekte /Informationen
		- Verschlüsselung von Zugängen zum Netzwerk und zu Netzverbindungen - Einsatz von Pseudonymen, Verfahren zur Pseudonymisierung von Daten. - Einsatz Verfahren zur Anonymisierung von Daten.						
06	**A.11** **Art 32 (1) b**	**Schutz von Gebäuden** Verhinderung des unautorisierten physischen Zugriffs auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung. Allgemeine Anforderungen: - Festlegung von Sicherheitsbereichen. - Realisierung des Zutrittsschutzes. - Festlegung zutrittsberechtigter Personen. - Verwaltung von personengebundenen Zutrittsberechtigungen. - Regelung zur Begleitung von Besuchern und Fremdpersonal. - Überwachung der Räume außerhalb der Schließzeiten. - Protokollierung des Zutritts.	x	x				x
07	**A.11** **Art 32 (1) b** **Art 32 (1) c**	**Schutz von Betriebsmitteln / Informationswerten** Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit der Organisation Allgemeine Anforderungen: - Sichere Platzierung von Betriebsmitteln. - Schutz vor Überspannung, Stromausfall, Wasser und Feuer. - Schutz vor Diebstahl. - Regelmäßige Wartung. - Prozess zur sicheren Löschung, Entsorgung und Vernichtung von Betriebsmitteln.	x	x				x
08	**A.12** **Art 32 (1) b**	**Betriebsverfahren und Zuständigkeiten** Sicherstellung des ordnungsgemäßen und sicheren Betriebes von Systemen und Verfahren zur Verarbeitung von Informationen. Allgemeine Anforderungen: - Dokumentation der Betriebsverfahren. - Härtung der Backend Systeme. - Getrennte Verarbeitung von Produktiv- und Testdaten. - Mandantenfähigkeit. - Aufgabenverteilung und Funktionstrennung von Funktionen, die nicht miteinander vereinbar sind.	x	x				

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrga verarbeitet werden)			**Formen der Zusammenarbeit**					
Nr	**Referenz ISO 27001/ DSGVO**	**Technisch-organisatorische Maßnahme**	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4. Remote-Zugriff bzw. Direktkopplung	5. System-Überlassung durch den Auftraggeber	6. Physische Objekte /Informationen
09	**A.12** **Art 32 (1) c**	**Datensicherungen:** Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Allgemeine Anforderungen: - Erstellen eines Datensicherungskonzeptes. - Durchführung regelmäßiger Datensicherungen. - Getrennte Aufbewahrung der Datensicherungsmedien.	x	x				
10	**A.12** **Art 32 (1) b**	**Schutz vor Malware und Patchmanagement** Verhinderung einer Ausnutzung technischer Schwachstellen durch Einsatz von aktueller Virenschutzsoftware und Implementierung eines Patchmanagements. Regelmäßiges Durchführen von Überprüfungen zur Erkennung von Schwachstellen. Allgemeine Anforderungen: - Regelmäßige Überwachung des Status von Sicherheitsupdates und Systemschwachstellen. - Einsatz von Anti-Malware-Software. - Regelmäßige Einspielen von Sicherheitspatches und Updates..	x	x	x	x		
11	**A.12** **Art 32 (1) d**	**Protokollierung und Überwachung** Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem (personenbezogene) Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind. (Sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens 3 Jahre lang durch den Auftragnehmer aufbewahrt.) Allgemeine Anforderungen: - Protokollierung der Berechtigungsvergabe und des Datenzugriffs. - Überprüfung von Benutzerberechtigungen. - Protokollierung der Aktivitäten und regelmäßige Auswertung der Benutzer- und Systemaktivitäten.	x	x		x		
12	**A.13** **Art 32 (1) b**	**Netzwerksicherheitsmanagement** Es muss ein angemessener Schutz für das Netzwerk implementiert werden, so dass die Informationen und die Infrastrukturkomponenten geschützt werden. Allgemeine Anforderungen: - Implementierung eines Netzwerkmanagements. - Benutzerauthentifizierung für externe Verbindungen und Verbindungen zwischen einzelnen Systeme. - Schutz der Diagnose- und Konfigurationsports. - Sicherheitsgateways an den Übergabepunkten / Netzgrenzen. - Isolation sensitiver Systeme.	x	x		x		

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrga verarbeitet werden)			**Formen der Zusammenarbeit**					
Nr	**Referenz ISO 27001/ DSGVO**	**Technisch-organisatorische Maßnahme**	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4. Remote-Zugriff bzw. Direktkopplung	5. System-Überlassung durch den Auftraggeber	6. Physische Objekte /Informationen
13	**A.13** **Art 32 (1) b**	**Informationsübertragung** Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten bzw. schutzbedürftiger Informationen und Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. (Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.) <u>Allgemeine Anforderungen:</u> - Sicherer Transport und Versand von Daten / Dokumenten in Abhängigkeit vom Schutzbedarf der Daten. - Protokollierung der Datenübertragungen. - Beschreibung von Schnittstellen zwischen Systemen und der externen Datenverbindungen. - Angemessener Schutz von Emails, die sensible Informationen / Daten beeinhalten. - Abschluss von Verträgen zum Schutz von Geschäftsgeheimnissen mit Dritten und Unterlieferanten.	x	x				
14	**A.13** **Art 32 (1) b**	**Netztrennung** Gruppen von Informationsdiensten, Mandanten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden. <u>Allgemeine Anforderungen:</u> - Logische Mandantentrennnung. - Datentrennung durch Segmentierung von Netzwerken unterschiedlicher Mandanten. - Trennung der Netze bei Remote Zugriffen.	x	x		x		
15	**A.14** **Art 25 (1)** **Art 25 (2)**	**Anschaffung, Entwicklung und Instandhaltung von Systemen** Maßnahmen, die sicherstellen, dass Informationssicherheit ein fester Bestandteil über den Lebenszyklus von Informationssystemen ist. <u>Allgemeine Anforderungen:</u> - Festlegung von sicherheitsspezifischen Regelungen und Anforderungen für den Einsatz neuer Informationssysteme und für die Erweiterung bestehender Informationssysteme. - Festlegung von Regelungen für die Entwicklung und Anpassung von Software und Systemen. - Leitlinien zur sicheren Systementwicklung.	x	x	x	x		

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrga verarbeitet werden)			**Formen der Zusammenarbeit**					
Nr	**Referenz ISO 27001/ DSGVO**	**Technisch-organisatorische Maßnahme**	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4. Remote-Zugriff bzw. Direktkopplung	5. System-Überlassung durch den Auftraggeber	6. Physische Objekte /Informationen
		- Überwachung von ausgelagerten Systementwicklungstätigkeiten. - Schutz von Testdaten.						
16	**A.15 Art 28)**	**Lieferantenbeziehungen bzw. Auftragsverarbeitung** Maßnahmen an die Informationssicherheit, zur Verringerung von Risiken, im Zusammenhang mit dem Zugriff von Lieferanten auf die Werte des Unternehmens, sollten mit Sublieferanten / Subunternehmern vereinbart und dokumentiert werden. Allgemeine Anforderungen: - Schriftliche Adressierung von Sicherheitsthemen in Verträgen mit Sublieferanten. - Festlegung von technisch organisatorischen Maßnahmen (TOMs) bei Verarbeitung personenbezogener Daten. - Überprüfung der Sicherheit bei Subunternehmern. - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten.	x	x	x	x	x	x
17	**A.16**	**Management von Informationssicherheitsvorfällen** Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall, Datenverlust etc.) zu implementieren. Allgemeine Anforderungen: - Prozesse zur unverzüglichen Information des Auftraggebers. - Protokollierung von Sicherheitsvorfällen. - Prozesse zur Behandlung und Vermeidung von Informationssicherheitsvorfällen.	x	x	x	x	x	x
18	**A.17 Art 32 (1) c**	**Informationssicherheitsaspekte des Business Continuity Management / Notfallmanagements** Die Aufrechterhaltung der Systemverfügbarkeit in schwierigen Situationen wie Krisen- oder Schadensfällen muss aufrechterhalten werden. Ein Notfallmanagement muss dieses sicherstellen. Die Anforderungen bezüglich der Informationssicherheit sollten bei den Planungen zur Betriebskontinuität und Notfallwiederherstellung festgelegt werden. Allgemeine Anforderungen: - Schaffung von Redundanzen. - Risikoabschätzung und Planung von Maßnahmen zur Sicherstellung des Geschäftsbetriebes. - Notfallpläne. - Regelmäßige Testes bzgl. der Wirksamkeit der Notfallmaßnahmen. - Frühzeitige Information des Auftraggebers bei Notfällen.		x				

Technisch-organisatorische Sicherheitsanforderungen in Abhängigkeit von der Form der Zusammenarbeit (Mit AV gekennzeichnete Maßnahmen sind nur relevant, wenn personenbezogene Daten im Auftrga verarbeitet werden)			**Formen der Zusammenarbeit**					
Nr	**Referenz ISO 27001/ DSGVO**	**Technisch-organisatorische Maßnahme**	1. Externe Datenbearbeitung	2. Datenverarbeitung auf Systemen des Auftragnehmers	3. Vor-Ort-Zugriff	4. Remote-Zugriff bzw. Direktkopplung	5. System-Überlassung durch den Auftraggeber	6. Physische Objekte /Informationen
19	**A.18 Art 32 (1) d**	**Einhaltung gesetzlicher und vertraglicher Anforderungen** Implementierung von Maßnahmen zur Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen sowie gegen jegliche Sicherheitsanforderungen. Allgemeine Anforderungen: - Geheimhaltungsverpflichtungen mit Mitarbeitern sowie Sublieferanten. - Sicherstellung der Einhaltung der gesetzlichen Verpflichtungen im Rahmen der Zusammenarbeit. - Rückgabe sämtlicher Daten, Betriebsmittel und Informationswerte an den Auftraggeber bei Vertragsende.	x	x	x	x	x	x
20	**A.18 Art 5**	**Datenschutzanforderungen und Datenschutzmanagement** Die Privatsphäre sowie der Schutz von personenbezogenen Daten sollten entsprechend den Anforderungen der relevanten Gesetze, Vorschriften und ggf. Vertragsbestimmungen sichergestellt werden. Allgemeine Anforderungen: - Bestellung eines Datenschutzbeauftragten. - Aufbau eines Datenschutzmanagements. - Erstellung von Verfahrensverzeichnissen. - Aufbau eines Datenschutznotfall Managements. - Durchführung regelmäßiger Überprüfungen / Audits. - Einhaltung der gesetzlichen Anforderungen im Rahmen der Auftragsdatenverarbeitung.	AV	AV	AV	AV	AV	
21	**A.18 Art 32 (1) d**	**Informationssicherheitsüberprüfungen** Es muss regelmäßig überprüft werden, ob die Informationsverarbeitung entsprechend der definierten Sicherheitsmaßnahmen durchgeführt wird. Hierfür wird der Auftragnehmer regelmäßige Prüfungen durchführen. Der Auftragnehmer räumt dem Auftraggeber das Recht ein, regelmäßige Prüfungen beim Auftragnehmer durchzuführen.	x	x	x	x	x	x