Nr.	Technische und organisatorische Maßnahmen (TOM) Art. 32 Abs. 1 DSGVO	Abschnitt	Inhalt
1	**1. Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)**	1.1.Zutrittskontrolle	Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten: –Sicherheitsschlösser mit Schlüsselregelung –verschlossene Türen bei Abwesenheit –Zutrittskontrollsystem (z.B. Ausweisleser, Magnetkarte, Chipkarte, Transponder unter Beachtung von kontrollierter Schlüsselvergabe) –Zutrittsregelungen für betriebsfremde Personen –Empfang, Werkschutz, Pförtner
2		1.2.Zugangskontrolle	Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern. Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung: –Erstellen von Benutzerprofilen –Einsatz von VPN-Technologie (auch bei Remote – Zugriffen) –Mobile Device Management –Identifizierung und Authentifizierung einschließlich Verfahrensregelungen zur Kennwortvergabe (Buchstaben, Groß.- Kleinschreibung, Mindestlänge, Zahlen, Sonderzeichen, regelmäßige systemseitige Aufforderung zum Wechsel des Kennworts) –Begrenzung der Fehlversuche –Protokollierung –Systemverwalterbefugnisse /-protokollierung –Dunkelschaltung des Bildschirms mit Passwortschutz bei Inaktivität –Firewall (Hardware-Firewall, Software-Firewall) –Virenschutz nach dem Stand der Technik –Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

3		1.3.Zugriffskontrolle	Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern: –Berechtigungskonzept mit differenzierten Berechtigungen –Verwaltung der Rechte durch Systemadministrator –Anzahl der Administratoren auf das „Notwendigste“ reduziert –Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten –Zugriffsprotokolle –Identifizierung und Authentifizierung –Aufbewahrung von Datenträgern in verschließbaren Schränken –physische Löschung von Datenträgern vor Wiederverwendung –ordnungsgemäße Vernichtung von Datenträgern (DIN 66399) –Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) –Protokollierung der Vernichtung
4		1.4.Trennungskontrolle	Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten. Maßnahmen zur getrennten Verarbeitung von Daten mit unterschiedlichen Zwecken: –Physikalische oder logische Trennung
5		1.5.Pseudonymisierung (Art. 32 Abs. 1 Buchst. a; Art. 25 Abs. 1 DSGVO)	Daten werden so verarbeitet, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer identifizierbaren betroffenen Person zugeordnet werden können; diese zusätzlichen Informationen werden gesondert aufbewahrt und sind durch technische und organisatorische Maßnahmen gesichert: –grundsätzlich keine (es werden Stammdaten verarbeitet) –im Rahmen der Gruppenverwaltung neu erzeugte Benutzernamen sind pseudonym (zufällig erzeugter Benutzername)

6	**2.Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)**	2.1.Weitergabekontrolle	Es ist zu gewährleisten, dass personenbezogene 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 durch Einrichtungen zur Datenübertragung vorgesehen ist: –Verschlüsselte Speicherung von Passwörtern –E-Mail-Verschlüsselung –Bereitstellung über verschlüsselte Verbindungen wie https, sftp –Sichere Verwahrung der zur Verschlüsselung verwendeten Schlüssel –Kennzeichnung der Datenträger –Bestandsverzeichnis und Bestandskontrolle der Datenträger –Festlegung der zur Abgabe von Datenträgern bzw. zur elektronischen Übertragung berechtigten Personen –Einrichtung eines VPN (Virtual Private Network) –Fernwartungskonzept
7		2.2.Eingabekontrolle	Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind: –Manuelle oder automatische Kontrolle der Protokolle –Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) –Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts –Klare Zuständigkeiten für Löschungen

8	**3.Verfügbarkeit, Belastbarkeit und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 Buchst. b und c DSGVO)**	3.1.Verfügbarkeit	Die Daten sind gegen zufällige und absichtliche Zerstörung oder Verlust zu schützen. Maßnahmen zur Datensicherung (physikalisch / logisch): –Backup-Verfahren (Festlegen von Rhythmus, Medium, Aufbewahrungszeit und -ort) –Spiegelung von Festplatten –Unterbrechungsfreie Stromversorgung (USV) –Betriebsbereitschaft –Notfallkonzept –Brandmelder –Feuersichere Türen –Virenschutz nach dem Stand der Technik –Firewall –Zusätzliche Sicherheitskopien mit Lagerung an besonders geschützten Orten –Erstellen eines Backup- & Recoverykonzepts –Testen von Datenwiederherstellung –Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
9		3.2.Belastbarkeit	Maßnahmen zur Sicherstellung der Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung: –Trennung zwischen Produktivsystem und Webserver/Mailserver –Intrusion Detection Systeme –Firewall (Hardware-Firewall, Software-Firewall) –Virenschutz nach dem Stand der Technik

10		3.3.Rasche Wiederherstellbarkeit	Maßnahmen zur Sicherstellung der raschen Wiederherstellbarkeit der Verfügbarkeit der personenbezogenen Daten und des Zugangs zu ihnen bei einem physischen oder technischen Zwischenfall: –Backup-Verfahren (Festlegen von Rhythmus, Medium, Aufbewahrungszeit und -ort) –Spiegelung von Festplatten –Unterbrechungsfreie Stromversorgung (USV) –Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenschutzverletzungen (auch im Hinblick auf die Meldepflicht gegenüber der Aufsichtsbehörde) –Einbindung bei Sicherheitsvorfällen und Datenpannen: Datenschutzbeauftragte Interne Sicherheitsbeauftragte
11	**4.Datenschutzmanagement, Auftragskontrolle, regelmäßige Überprüfung (Art. 32 Abs. 1 Buchst. d DSGVO)**	4.1.Datenschutzmanagement	–Datenschutzverantwortliche intern –Regelprozesse mit kurzfristiger Reaktionszeit auch außerhalb der Regelarbeitszeiten (nachts, Wochenende, Feiertage) –Externer Datenschutzbeauftragter
12		4.2.Auftragskontrolle	Die weisungsgemäße Auftragsverarbeitung ist zu gewährleisten. Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer: –Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung –Schriftliche Festlegung der Weisungen –Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit) –Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis –Festlegung von turnusgemäßen Kontrollen des Auftragnehmers durch den Auftraggeber –Regelmäßige interne Kontrolle und Dokumentation des Auftragnehmers, dass Weisungen und Regelungen zur Auftragsdurchführung beachtet werden

13		4.3.Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	–Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …) –Regelmäßige Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen –Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet –Bedarfsgerechte Sensibilisierung der Mitarbeiter –Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt –Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach –Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

14	**1. Zutrittskontrolle zu den Arbeitsbereichen (TOM ANLAGE 2)**	1.1.Organisation der Zutrittskontrolle	–Schlüssel-Regelungen –Zugangsregelungen für betriebsfremde Personen –Empfang –Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.) Entwicklungsdienstleister: –Festgelegte Sicherheitsbereiche –Zutrittsberechtigungskonzept –Individuelle Zutrittsberechtigungsvergabe –Dokumentation von Zutrittsberechtigungen –Zutrittsdokumentation –Besucherregelungen Rechenzentren: –Festgelegte Sicherheitsbereiche –Alarmmeldesystem mit Aufschaltung eines Sicherheitsdienstes –Definierter Prozess zu Zutrittsberechtigungsvergabe und -entzug –Individuelle Zutrittsberechtigungsvergabe –Dokumentation von Zutrittsberechtigungen –Zutrittsdokumentation –Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal, etc.) –Autorisiertes Wachpersonal (RZ1, FFM) –Ständig besetzte Notrufzentrale (RZ1, FFM) –Protokollierung der Besucher

15		1.2. Allgemeine Gebäudesicherheit	–Sicherheitsschlösser –Büroräume sind außerhalb der Arbeitszeit verschlossen –Separate Brandabschnitte Entwicklungsdienstleister: –Manuelles Schließsystem –Sicherheitsschlösser mit Schlüsselregelung –Büroräume sind außerhalb der Arbeitszeit verschlossen –Separate Brandabschnitte Rechenzentren: –Elektronische Schließsystem (NOC, Offenbach) –Sicherheitstüren (RZ1, FFM und RZ2, FFM) –Serverraum ist fensterlos, abgeschlossen und alarmgesichert (RZ1, FFM und RZ2, FFM)

16		1.3.Technische Sicherheitsmaßnahmen	–Schutz und Beschränkung der Zutrittswege –Zutrittskontrollsystem mit Transponder-, Code- oder schlüsselkartenbasierter Schließanlage Entwicklungsdienstleister: –Zutrittskontrollsystem –Transponder-, Code- oder schlüsselkartenbasierte Schließanlage Rechenzentren: –Transponder-, Code- oder schlüsselkartenbasierte Schließanlage (NOC, Offenbach) –Perimeter-System (RZ1, FFM) –Schutz und Beschränkung der Zutrittswege (RZ1, FFM) –Bewegungsmelder (RZ1, FFM) –Video-Überwachung (RZ1, FFM) –Betreten und Verlassen des Serverraums wird elektronisch protokolliert und mittels Videoaufzeichnung aufgezeichnet (RZ1, FFM) –Zutrittskontrollsystem –Zusätzliche Zugangsbeschränkung der Serverräume –Vereinzelungsanlage mit Fingerabdrucksensor (RZ2, FFM) –Verschlossene Serverracks –Separat gesicherter Serverraum im RZ –Gehäuseschlösser

17	**2. Zugangskontrolle zu Datenverarbeitungssystemen**	2.1Hardware- und Netzwerk-Sicherheitsmaßnahmen	–Schutz der Infrastruktur durch Hardware-Firewalls –VPN-Beschränkungen –Externer Zugang nur über sichere Verbindungen (VPN, RDP oder vergleichbar) –Schutz der Infrastruktur durch Intrusion Detection-Systeme –Protokollierung von benutzerrelevanten Aktivitäten (Anmeldung, Abmeldung, Zugangsverweigerungen, etc.) Entwicklungsdienstleister: –VPN-Beschränkungen –Schutz der Infrastruktur durch Intrusion Response-Systeme –Segmentierung des Netzwerkes –Festplattenverschlüsselung Rechenzentren: –Segmentierung des Netzwerkes durch VLANs –Demilitarisierte Zonen –VPN-Beschränkungen –Externer Zugang nur über sichere Verbindungen und über passwortgeschützte, verschlüsselte authentifizierte Verbindungen (VPN, RDP oder vergleichbar) –Schutz der Infrastruktur durch Hardware-Firewalls –Client-Zertifikate für Schutz vor unberechtigtem Zugang –Festplattenverschlüsselung –Nicht benötigte physikalische Schnittstellen sind deaktiviert –Nicht benötigte Dienste sind gesperrt –Portregeln/Sperrung von nicht erforderlichen Ports –Verschlüsselung von Systemen oder virtualisierten Instanzen –Systemhärtungsvorgaben, wie etwa Deaktivierung nicht erforderlicher Komponenten bzw. Funktionen

18		2.2Hardware- und Netzwerk-Sicherheitsmaßnahmen	–Software-Firewall –Antivirus-Software auf allen Systemen –Automatische Bildschirm- und Computer-Sperre bei Inaktivität –Verschlüsselte Speicherung von Passwörtern –Regelmäßige Software-Updates Rechenzentren: –Verschlüsselte Speicherung von Passwörtern –Software-Firewall –Antivirus-Software auf allen Systemen –Verschlüsselungsmechanismen –Automatische Sitzungsbeendigung bei Inaktivität –Automatische Bildschirm- und Computer-Sperre bei Inaktivität

19		2.3Benutzerzugangsbeschränkungen	–Rollenbasierte Benutzerprofile –Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich –Erforderliche Mindestkomplexität für Kennwörter –Zwangs- oder Pflicht-Änderung der Benutzerkennwörter nach der erstmaligen Systemanmeldung –Ablauf von Benutzerpasswörtern –Automatische Deaktivierung von Benutzern nach mehreren fehlgeschlagenen Logins –User-Login-Verlauf –Überwachung und Protokollierung von administrativem Systemzugang und von Konfigurationsänderungen Rechenzentren: –Temporäre Benutzerauthentifizierung für Systemzugang- und/oder Anwendungszugriff erforderlich –Verschlüsselte Speicherung von Passwörtern in zentralem Passwortsafe Zugriff wird protokolliert und überwacht Passwörter können mit Siegel und Siegelbruchkontrolle versehen werden –Einschränkung der zeitlichen Gültigkeit der Benutzerkonten –Zwangs- oder Pflicht-Änderung der Benutzerkennwörter –Erforderliche Mindestkomplexität für Kennwörter –Passwort-Historie zur Verhinderung der Mehrfachnutzung desselben Passwortes –Angemessene Gestaltung der Benutzeraccount-Wiederherstellung im Falle eines verlorenen oder vergessenen Authentifizierungsdatensatzes –Berechtigungen bzw. -änderungen werden protokolliert und regelmäßig überprüft

20		2.4Organisatorische Sicherheitsmaßnahmen	–Geregelte Vergabeverfahren für Systemzugriffsberechtigungen –Regelmäßige Überprüfung der Systemzugangsberechtigungen –Deaktivierung von nicht benötigten Accounts –Anzahl der Administratoren auf das Notwendigste beschränkt Rechenzentren: –Vertraulichkeitserinnerungen –Wartung und Aktualisierung der Sicherheitssysteme nach aktuellem Stand der Technik und der Kenntnis über (neue) Schadsoftware

21	**3. Zugriffskontrolle auf bestimmte Bereiche der Datenverarbeitungssysteme**	3.1Organisatorische Sicherheitsmaßnahmen	~~Rollenbasiertes Berechtigungskonzept mit minimal notwendigen~~ Zugriffsrechten –Zentrale Verwaltung der Benutzerrechte durch Systemadministratoren –Beschränkung der Administrationsrechte auf das erforderliche Maß –Minimierung der Personen mit Administrationsberechtigung –Authentifizierung für den Daten- oder Anwendungszugriff erforderlich –Regeln für die sichere Lagerung von physikalischen Datenträgern –Geregeltes Löschen bzw. Vernichten und Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB-Sticks –Vernichtung von physikalischen Medien nach DIN 66399 oder vergleichbaren Standards –Dokumentation der Datenträgervernichtung bzw. -löschung Entwicklungsdienstleister: –Minimierung der Personen mit Administrationsberechtigung –Clean Desk Policy Rechenzentren: –Rollenbasiertes Berechtigungskonzept mit minimal notwendigen Zugriffsrechten (Lesen / Schreiben / Ändern / Kopieren / Löschen) –Zugang zu IT-Systemen erhalten nur Mitarbeiter, die ausreichend geschult wurden und über fachliche Qualifikation verfügen (wird durch Ausbildungen, Weiterbildungen, Berufserfahrung und Bewertungen durch Fachabteilungen sichergestellt) –Geregeltes Löschen bzw. Vernichten und Entsorgen von Datenträgern wie Festplatten, USB-Sticks –Vernichtung von physikalischen Medien durch zertifiziertes Unternehmen unter Aufsicht von Mitarbeitern sowie Protokollierung –Dokumentation der Vergabe von Zugriffsrechten –Standardisiertes Verfahren für Erteilung und Entzug von Zugriffsrechten –Regeln für die sichere Lagerung von physikalischen Datenträgern

22		3.2Technische Sicherheitsmaßnahmen	–Netzwerkzugangskontrolle –Trennung von Anwendungs- und Administrationszugängen –Überwachung und Protokollierung allgemeiner Benutzeraktivität (Datenzugriff, Datenexport, Datenlöschung) –Zugriffsprotokollierung –Nutzung eines Aktenvernichters mit ausreichender Sicherheitsstufe (vgl. DIN 66399) –Verbot/Unterbindung von nicht autorisierten Software-Installationen Rechenzentren: –Personalisierte Zugänge für autorisierte Mitarbeiter in Kundenprojekte zur Erfüllung der SLAs –Zugriffe auf die IT-Systeme werden im Access-Log protokolliert und je nach Projektanforderung aufbewahrt –Relevante Dienste auf IT-Systemen (Konsole, Datenbanken, Webserver) werden in Form von Log-Files protokolliert (Nutzer, die personenbezogene Daten verarbeiten, erhalten keinen Zugriff auf die Logfiles) –Schnittstellen und Übertragungswege von einem IT-System zu anderen IT-Systemen definiert –Verschlüsselung von Datenübertragungsvorgängen –Regelmäßige Sicherheits-Updates

23	**4. Weitergabe von personenbezogenen Daten (Weitergabekontrolle)**	4.1Technische Sicherheitsmaßnahmen	–Verschlüsselung von Daten während der Übertragung (end-to-end-Verschlüsselung) –E-Mail-Verschlüsselung Entwicklungsdienstleister: –Sichere Transportbehältnisse für Datenträger Rechenzentren: –Personenbezogene Daten werden ausschließlich signiert, verschlüsselt und passwortgeschützt per Gnu/PGP versendet (Verschlüsselung und Signierung ebenfalls bei physischem Versand) –Verschlüsselung von Daten während der Übertragung (SSL, TLS, IPSec und VPN) –Verwendung von Einmalpasswörtern zur Entschlüsselung von übertragenen Daten; Schlüssel wird auf separaten Übertragungsweg übergeben –Dokumentation bzw. Protokollierung von externen Support-Prozessen

24		4.2Organisatorische Maßnahmen	–Verwaltung und Dokumentation von physischen Speichermedien –Weitergabe von pseudonymisierten Daten –Verbindliche Regeln für die Offenlegung von sensiblen Daten –Regelungen für die Weitergabe von Datenträgern Entwicklungsdienstleister: –Dokumentation der Weitergabe von physischen Speichermedien –Regelungen für die Aufbewahrung von Datenträgern Rechenzentren: –Datentransfer und -weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers –Vollständige Löschung aller Datenkopien und Datensicherungen nach Abschluss des Auftrags –Datentransfer und -weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers –Verbot der Nutzung von privaten Datenträgern –Keine Speicherung von personenbezogenen Daten dauerhaft auf mobilen Datenträgern –Regelungen für die Verschlüsselung von Daten –Schriftliche Richtlinien für die Datenübertragung und -weitergabe –Dokumentation der Weitergabe von physischen Speichermedien –Festplatten, die nicht mehr im vorgesehenen Kundenprojekt verwendet werden (RMA, Austausch, Projektende) werden in einer eigenen Shredderstation durch 7-maliges Überschreiben dauerhaft gelöscht –Ausdrucke und CDs, die Kunden-, System- oder personenbezogene Daten enthalten, werden in einer Dokumentenvernichtungstonne gesammelt und durch ein zertifiziertes Fachunternehmen nach Sicherheitsstufe P-4 / DIN 663399-1 vernichtet

25	**5. Überprüfbarkeit der Datenverarbeitung (Eingabekontrolle)**	5.1Technische Maßnahmen	–Applikationsbasierte Überprüfung der Eingabeberechtigung –Rollenabhängige Eingabebeschränkungen und Schutz gegen nicht autorisierte Veränderungen –Protokollierung von administrativen Änderungen –Änderungsprotokollierung auf Datensatz- und Nutzerebene –Protokollierung der relevanten Prozesse (Speicherung, Verarbeitung, Modifizierung, Abrufen, Übertragung, Löschung, etc.)
26		5.2Organisatorische Maßnahmen	–Definition von Rollen für unterschiedliche Aufgaben –Aufteilung der Zuständigkeiten –Regelmäßige Analyse der Protokolldateien Entwicklungsdienstleister, Rechenzentren: –Vertragliche Beschränkungen der Zahl der Beschäftigten mit Zugriff auf personenbezogene Daten –Aufteilung der Zuständigkeiten
27	**6.Sicherstellung der weisungskonformen Datenverarbeitung (Auftragskontrolle)**	6.1Organisatorische Maßnahmen	–Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers –Sorgfältige Auswahl von Auftragnehmern –Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation –Auftragsverarbeitungsverträge mit Auftragnehmern –Auftragsverarbeitungsverträge der Auftragnehmer mit Unterauftragnehmern –Verpflichtung der Auftragnehmer und Unterauftragnehmer auf das Datengeheimnis –Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer –Regelungen zum Einsatz weiterer Subunternehmer –Überprüfung/Auditierung von Auftragnehmern –Regelmäßige Kontrolle externer Dienstleister –Datenvernichtung nach Vertragsende –Dokumentierte interne Kontrollen des Auftragnehmers zur Sicherstellung der weisungskonformen Verarbeitung personenbezogener Daten

28		6.2 Technische Maßnahmen	–Fern-Zugriff erfolgt nur mit starker Verschlüsselung, erfordert eine Benutzerauthentifizierung und unterliegt strikten Regeln zur Zugriffsbeschränkung –Mechanismen zur Prävention von nicht autorisiertem Datenzugriff durch Mitarbeiter des Auftragnehmers
29	**7.Gewährleistung der Verfügbarkeit von Datenbeständen und Datenverarbeitungsanlagen (Verfügbarkeitskontrolle)**	7.1 Technische Maßnahmen	–Unterbrechungsfreie Stromversorgung –Redundante Datenspeicherung –RAID-System/Festplattenspiegelung –Desaster-Recovery-Mechanismen für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust –Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen –Physikalisch getrennte Systeme für unterschiedliche Zwecke Rechenzentren: –Schutz gegen DDoS und weitere bekannte Cyberangriffe (Vergleich OWASP) –Dedizierte Firewalls sowie Firewall-Cluster –Unterbrechungsfreie Stromversorgung –F90 Brandschutzabschnitte, -wände und -türen –Brand- und Rauchmeldeanlagen –Gaslöschanlagen –Notstromaggregate –Redundante Versorgungsdienste –Überspannungsschutz –Kühlsystem im Rechenzentren/Serverraum –Load Balancing durch mehrere parallel arbeitende Systeme –Tägliche inkrementelle Datensicherung

30		7.2Organisatorische Maßnahmen	–Backup- und Wiederherstellungskonzept –Notfall- und Wiederherstellungspläne sind vorhanden –Business Recovery Plan (BRP) vorhanden, um Ausfall der IT-Infrastruktur vorzubeugen –Brandmelder (mit Feuerwehraufschaltung) –Räumlich getrennte Archivierung –Regelmäßige Funktionstests –Test der Datenwiederherstellung –Physikalisch getrennte Systeme für unterschiedliche Zwecke Rechenzentren: –Notfallpläne sind vorhanden –Regelmäßige Funktions- und Notfalltests werden durchgeführt –Schwachstellen-Scans –Regelmäßige Web-Application- und Server-Vulnerability-Scans –Zeitnahes Einspielen von Patches –Auftraggeber wird über Störungen des Betriebes schnellstmöglich in Kenntnis gesetzt oder kann direkt an das Monitoring angebunden werden –CMDB zum Überblick und Identifikation aller eingesetzten Systeme, inklusive der Bestimmung ihrer Hardware-, Software- und Firmware-Versionen –Regeln für die Aufbewahrung von Schlüsseln zur Entschlüsselung von Daten oder zur Verifizierung digitaler Signaturen –Brandmelder –Zentrale Datenhaltung –Automatische Systemüberwachung und Benachrichtigung der Administratoren bei Irregularitäten
31	**8.Trennung von unterschiedlichen Datenbeständen (Trennungskontrolle)**	8.1 Technische Maßnahmen	–Mandantenfähigkeit von Anwendungen –Physikalische Datentrennung: Getrennte Computersysteme oder Medien Rechenzentren: –Physikalische Datentrennung: Getrennte Computersysteme oder Medien –Separate Instanzen für Entwicklungs- und Produktivsystemen (Sandboxes)

32		8.2Organisatorische Maßnahmen	–Logische Datentrennung –Keine Nutzung von Produktivdaten zu Testzwecken –Datenfelder in Anwendungen sind mit zweckbestimmenden Attributen versehen worden Rechenzentren: –Strukturierte Dateiablage –Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff –Abschottung der unterschiedlichen Projekte durch unterschiedliche Zugriffsrechte
33	**9.Verschleierung von Daten und Entfernung von Bezügen**		–Pseudonymisierung der Daten auf Datenbankebene –Getrennte Aufbewahrung des Pseudonyms und der zur Identifizierung notwendigen Daten –Maskierung von Daten auf Anwendungsebene –Aufhebung von Personenbezügen auf Anwendungsebene
34	**10.Datenschutz-Management**	10.1Regulatorische Anforderungen	–Benennung eines Datenschutzbeauftragten –Benennung von internen Datenschutzkoordinatoren –Schriftliche Verpflichtung aller Mitarbeiter auf das Datengeheimnis –Regelmäßige Schulungen der Mitarbeiter zu Datenschutz und Datensicherheit –Verzeichnis für Verarbeitungstätigkeiten wird fortlaufend aktualisiert –Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung –Konzept zur Datenlöschung –Dokumentierter Prozess zur Erkennung und Meldung von Datenschutzverstößen und Datensicherheitsvorfällen –Prozess zur Wahrnehmung von Betroffenenrechten (insbesondere Informations- und Auskunftspflichten) –Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind –Nachweise über Datenschutz-Folgenabschätzungen

			Regelmäßige Abstimmung mit dem Datenschutzbeauftragten –Mobile Device Management –Verwaltungsverfahren für kryptographische Schlüssel –Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung (Wiki, Intranet, etc.) –Anlassbezogene Schulungen oder Informationen der Mitarbeiter –Datenschutz- oder sonstige Compliance-Audits –Datenschutz und Datensicherheitsrichtlinien –Disziplinarmaßnahmen im Falle einer Datenschutzverletzung –Zumindest dreistufige Klassifizierung von Daten (öffentlich, intern, vertraulich) –Verbindliche Vorgaben für Administratoren –Dokumentation und Prüfung über Hard- und Softwareänderungen (Evaluation vor und nach der Änderung) –Unterschiedliche Zuständigkeiten für Anfrage, Genehmigung und Implementierung von Hard- und Softwareänderungen –Software-Lebenszyklus-Management (SDLC) –Schriftliche Richtlinien und zusätzliche Maßnahmen für mobiles Arbeiten und Home Office –Schriftliche Dokumentation der Endgeräteverwaltung Entwicklungsdienstleister: –Geeignetes Informationssicherheitssystem (ISMS) gemäß anerkannten Standard wie etwa ISO/IEC 27001 vorhanden –Betrieb der Infrastruktur in ISO/IEC 27001-zertifiziertem Rechenzentrum erstreckt –BYOD-Vereinbarung Rechenzentren: –Benennung von IT-Compliance-Beauftragten
35		10.2Organisatorische Maßnahmen	