Technische und organisatorische Maßnahmen
der GrantLift GmbH
(Stand: 09/2026)

§ 1 Allgemeine Informationen

Dieses Dokument ist Teil der Datenschutzdokumentation des Datenschutzmanagementsystems. Diese Version des Dokumentes ersetzt alle früheren Versionen und Ausgaben.

§ 2 Allgemeines zur Organisationsstruktur

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Wird das Thema Informationssicherheit bei allen Prozessen mitgedacht?	x ja □ nein	RiLi Privacy by Design & Default
2.	Sind Sicherheitsricht- und -leitlinien definiert, von der Geschäftsleitung genehmigt und dem Personal kommuniziert?	x ja □ nein	Leitlinie zur Informationssicherheit und zum Datenschutz
3.	Werden regelmäßige Überprüfungen der Wirksamkeit der technischen und organisatorischen Maßnahmen durchgeführt?	x ja □ nein	Verfahren zur regelmäßigen Überprüfung VV und TOMs
4.	Werden Konzepte und Dokumentationen im Sicherheitsumfeld regelmäßig überprüft und aktuell gehalten?	x ja □ nein	gemeinsam mit dem Datenschutz-beauftragten (***DSB***)
5.	Wird je nach Unternehmensgröße ein geeignetes Informationssicherheits-managementsystem (***ISMS***) eingesetzt?	□ ja x nein	Derzeit nicht (kleines Unternehmen)
6.	Sind die Rollen und Verantwortlichkeiten im Bereich der Sicherheit im eigenen Betrieb bekannt und besetzt, einschließlich des Informationssicherheitsbeauftragten (***ISB***), IT-Leiters und DSB?	x ja □ nein	ISB = Gabriel Kienberger
7.	Wird der DSB konsequent bei Sicherheitsfragen einbezogen?	x ja □ nein	
8.	Verfügt der DSB über ausreichende fachliche Qualifikation für sicherheitsrelevante Frage-stellungen und besteht die Möglichkeit zur Fortbildung in diesem Bereich?	x ja □ nein	DSB ist Fachanwalt für Informations-technologierecht mit Fortbildungspflicht
9.	Werden regelmäßige Audits des DSB gemäß Art. 32 DSGVO zur Sicherheit der Verarbeitung durchgeführt?	x ja □ nein	
10.	Sind die zuständige Datenschutz-aufsichtsbehörde sowie die Meldever-pflichtungen nach Art. 33 und 34	x ja □ nein	Richtlinie Vorgehen bei Datenschutz-verletzungen

	DSGVO (***Verletzung der Sicherheit***) bekannt?		
11.	Existieren Eskalationsprozesse bei Sicher-heitsverletzungen, inklusive der klaren Information darüber, wer wann wie zu informieren ist, insbesondere im Notfall-management?	x ja □ nein	Notfallplan
12.	Werden Sicherheitsvorkommnissen konse-quent dokumentiert (***Security Reporting***)?	x ja □ nein	Beim Unternehmen und DSB
13.	Wird die Zusammenarbeit zwischen dem DSB und dem ISB aktiv durch die Unternehmens-leitung unterstützt?	x ja □ nein	
14.	Werden Erkenntnisse über (neue) digitale Bedrohungen gesammelt und werden potentielle Auswirkungen auf den eigenen Betrieb abgeleitet?	x ja □ nein	Bitdefender - Schadsoftware Erkennung

§ 3 Schutz der Infrastruktur vor Eingriffen Unbefugter und vor Naturereignissen

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Besteht ein Gesamtkonzept zur Gebäude-sicherung im Allgemeinen, einschließlich Brandschutz, Zutrittsbeschränkung und Zutrittskontrolle?	x ja □ nein	vermieterseits
2.	Existiert ein Konzept zu Zutrittsregelungen und zur physischen Zugangskontrolle?	x ja □ nein	vermieterseits
3.	Gibt es klare Regelungen zum Umgang mit Besuchern als Bestandteil des Konzepts, einschließlich Begleitung, Sicherheitszonen, Besucherausweise, Protokollierung und einem zuständigen Mitarbeiter für Besucher?	x ja □ nein	Nur begleitete Besuche
4.	Sind Regelungen zum Umgang mit externen Dienstleistern (z. B. Werkverträge, Handwerker, Wartung von Systemen) vor-handen, wie Verschwiegenheitserklärungen, persönliche Begleitung in Sicherheitszonen oder Protokollierung?	x ja □ nein	Nur begleitete Dienstleister
5.	Wurden verschiedene Sicherheitszonen geschaffen?	x ja □ nein	Besucherbereich separat
6.	Gibt es eine aktuelle Übersicht zur Berechtigungsverwaltung in Sicherheitszonen (Welcher Mitarbeiter darf in welche Zone)?	x ja □ nein	Nur für Besucher

7.	Wird der Zugang zu Sicherheitszonen durch geeignete Technik begrenzt?	□ ja x nein	
8.	Werden selbstschließende Türen bei Zonenübergängen in Sicherheitszonen eingesetzt?	□ ja x nein	
9.	Sind sichere Schließsysteme mit dokumentierter Schlüsselverwaltung implemen-tiert?	x ja □ nein	vermieterseits
10.	Gibt es ein Brandschutzkonzept?	x ja □ nein	vermieterseits
11.	Werden Feuer-/Rauchmeldeanlagen im Rahmen des Brandschutzkonzepts verwendet?	x ja □ nein	vermieterseits
12.	Gibt es den Einsatz von automatischen Löschsystemen in Serverräumen?	□ ja x nein	
13.	Werden feuerhemmende Schränke/Tresore zur Lagerung essentieller Komponenten (z. B. Backup-Bänder, wichtige Originaldokumente) verwendet?	□ ja x nein	
14.	Werden Gebäude (z. B. Wände, Fenster) und Infrastruktur (z. B. Leitungen, Gefahren-meldeanlagen) regelmäßig geprüft und gewartet?	x ja □ nein	vermieterseits
15.	Falls ein Betriebsgelände existiert: Ist das Betriebsgelände umzäunt?	□ ja x nein	Kein Betriebsgelände
16.	Gibt es stabile, einbruchhemmende Fenster und Türen im Erdgeschoss?	□ ja x nein	4. OG
17.	Werden Alarmanlagen zur Einbruchserkennung eingesetzt, insbesondere außerhalb der Arbeitszeit?	x ja □ nein	vermieterseits
18.	Gibt es den Einsatz von Sicherheitspersonal (ggf. extern)?	x ja □ nein	vermieterseits
19.	Wird Videoüberwachung unter Berück-sichtigung datenschutzrechtlicher Anforder-ungen eingesetzt, insbesondere für das Monitoring des Zugangsschutzes?	□ ja x nein	
20.	Ist eine ausreichende Klimatisierung von Serverräumen gewährleistet?	□ ja x nein	Keine eigenen Server
21.	Gibt es keine (zu öffnenden) Fenster in Serverräumen?	□ ja x nein	

22.	Wird eine unterbrechungsfreie Stromver-sorgung für Serversysteme eingesetzt (bei kurzfristigen Stromausfällen oder Schwan-kungen)?	□ ja x nein	
23.	Wird Elementargefahren (insbesondere Feuer, Rauch, Erschütterungen, chemische Reaktionen, Überschwemmungen, Stromausfälle, Explosionen, Anschläge/Vandalismus) vorgebeugt?	□ ja x nein	
24.	Wurden Risiken durch Überflutung/Starkregen geprüft, insbesondere bei Serverräumen im Keller oder in anderen gefährdeten Bereichen?	□ ja x nein	

§ 4 Schulung der Beschäftigten

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Erhält das gesamte Personal eine Schulung für Informationssicherheit und Datenschutz, soweit dies für die jeweilige Funktion relevant ist?	x ja □ nein	Schulung über DSB
2.	Werden Datenschutzschulungen für neue Beschäftigte zeitnah nach Aufnahme des Beschäftigungsverhältnisses durchgeführt?	x ja □ nein	s.o.
3.	Erfolgen regelmäßige Auffrischungs-schulungen für bestehendes Personal, beispielsweise einmal pro Jahr?	x ja □ nein	s.o.
4.	Erhalten alle Personen im Betrieb regelmäßige Informationen über Neuigkeiten zum Datenschutz und der IT-Sicherheit?	x ja □ nein	z. B. per Mail, Slack
5.	Werden relevante Richtlinien, wie zur E-Mail-/Internetnutzung, Umgang mit Schadcode Meldungen und Einsatz von Verschlüssel-ungstechniken, aktuell gehalten und sind leicht auffindbar?	x ja □ nein	Sicherheitsrichtlinie E-Mail- und Internet-nutzung, KI-Richtlinie, Passwortrichtlinie, etc.
6.	Sind die Präsentationen mit den Schulungs-inhalten zugänglich für alle betroffenen Mitarbeiter?	x ja □ nein	
7.	Kennen ausgewählte Mitarbeiter, die bei der Erkennung von Sicherheitsverletzungen beteiligt sind, die internen Prozesse zum Umgang mit Vorfällen, einschließlich Meldung nach Art. 33 DSGVO und Notfallplan?	x ja □ nein	Richtlinie Vorgehen bei Datenschutz-verletzungen, Notfallplan

8.	Wird in den Schulungsinhalten vermittelt, wie Cyberangriffe mittels Social-Engineerings eingeleitet werden?	x ja □ nein	
9.	Erfahren die Beschäftigten in den Schulungsinhalten von den Gefahren der E-Mail-Kommunikation, insbesondere bei verschlüsselten E-Mail-Anhängen (z. B. Zip-Datei mit Passwort)?	x ja □ nein	
10.	Werden in den Schulungsinhalten die Beschäftigten darin geschult, gefälschte E-Mails zu erkennen, z. B. durch Überprüfung von Absenderadressen, Auffälligkeiten und eingebetteten Links?	x ja □ nein	
11.	Erfolgt eine Sensibilisierung des Personals, das mit Externen wie Lieferanten interagiert, hinsichtlich Richtlinien, Prozessen und Verhalten, einschließlich dessen, welche Daten in welcher Form weitergegeben werden dürfen und was sicherheitskritisch sein kann?	x ja □ nein	
12.	Wird den Mitarbeitern, die von Heimarbeit betroffen sind, die sichere Nutzung von Home Office Lösungen erläutert und werden spezifische Gefahren aufgezeigt?	x ja □ nein	RiLi Mobiles Office

§ 5 Authentifizierung

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Wird das gesamte Personal in den Umgang mit Authentifizierungsverfahren und -mechanismen eingewiesen?	x ja □ nein	
2.	Existiert ein geregelter Prozess zur zentralen Verwaltung von Benutzeridentitäten, insbesondere zur Anlage (z. B. neuer Mitarbeiter), Änderung (z. B. Namenswechsel nach Heirat) und Löschung (z. B. Weggang Mitarbeiter)?	x ja □ nein	Richtlinie zum Berechtigungsmanage-ment; Sicherheitsrichtlinie für IT-Administratoren
3.	Werden eindeutige Kennungen für jeden Nutzer vergeben und erfolgt die Vermeidung von Gruppenkennungen?	x ja □ nein	Grundsätzlich ja, Werkstudenten werden einer bestehenden Lizenz zugeordnet
4.	Falls Gruppenkennungen zwingend verwendet werden: Wird eine datenschutz-konforme Protokollierung der dazugehörigen Nutzeraktivitäten eingesetzt?	x ja □ nein	Grundsätzlich ja, Werkstudenten werden einer bestehenden Lizenz zugeordnet

5.	Wird die Vergabe von starken Passwörtern gefördert und eine Richtlinie dafür veröffentlicht?	x ja □ nein	Passwortrichtlinie
6.	Erfolgt die automatische Umsetzung der Passwortrichtlinie für starke Passwörter in den Systemen mit Nutzerkennungen?	x ja □ nein	Über Passwortrichtlinie
7.	Wird die Auswahl schwacher Passwörter bei Anwendungen verhindert?	x ja □ nein	Über Passwortrichtlinie
8.	Gibt es eine Überprüfung der Umsetzung der Regel, dass Passwörter nach festgelegten Zeiträumen (z. B. 60 Tage) geändert werden müssen?	□ ja x nein	Passwortwechsel nur bei Verdacht von potentiellen Fremdzugriffen oder bei möglichem Verlust von BK und PW; vgl. Passwortrichtlinie
9.	Werden Passwörter nach einem Sicherheits-vorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden?	x ja □ nein	
10.	Muss beim erstmaligen Login eines neuen Nutzers oder bei Zurücksetzung des Passworts durch die IT (z. B. bei Vergessen des Passworts) eine Passwortänderung durch den Nutzer erfolgen?	x ja □ nein	
11.	Ist es den Beschäftigten untersagt, Passwörter weiterzugeben (auch nicht an Kollegen, Vorgesetzte oder die IT-Abteilung) und wird im Ausnahmefall (z. B. längere Erkrankung) das Passwort durch die IT zurückgesetzt, wobei dieser Vorgang dokumentiert wird?	x ja □ nein	Über Passwortrichtlinie
12.	Wurden die Beschäftigten darüber informiert, dass Passwörter nicht auf Zettel oder Pinnwänden aufgezeichnet werden dürfen?	x ja □ nein	Über Passwortrichtlinie
13.	Wird die Speicherung von Passwörtern im Browser ohne Sicherung durch ein Masterpasswort vermieden?	x ja □ nein	
14.	Wird die Mehrfachverwendung eines Passworts für verschiedene Dienste vermieden, sofern kein zentrales Identitätsmanagement (z. B. Active Directory) verwendet wird?	x ja □ nein	Passwortmanager soll immer verwendet werden
15.	Wird verhindert, dass Passwörter per E-Mail übermittelt werden (z. B. für einen Firmenaccount zu einem Cloud-Dienst)?	x ja □ nein	

16.	Werden für lokale Admin-Konten besonders starke Passwörter verwendet?	x ja □ nein	
17.	Wird Zwei- oder Mehr-Faktor-Authentifi-zierung eingesetzt?	x ja □ nein	
18.	Wird konsequent die Zwei-Faktor-Authenti-fizierung für Admin-Konten eingesetzt?	x ja □ nein	bei den datenschutzrelevanten Accounts
19.	Wird eine automatische Sperrung von Zugängen bei zu vielen Fehlversuchen durch falsches Passwort implementiert (entweder zeitbasiert oder komplett, wobei in letzterem Fall eine Kontaktaufnahme mit der IT notwendig ist)?	x ja □ nein	bei den datenschutzrelevanten Accounts
20.	Gibt es eine Zeitverzögerung zwischen einzelnen Login-Versuchen (insbesondere bei über das Internet erreichbaren Anwendungen) zur Erschwerung von automatischen Online-Angriffen?	x ja □ nein	bei den datenschutzrelevanten Accounts
21.	Wird die Anzahl der fehlgeschlagenen Logins für einen Nutzer, der sich erfolgreich anmeldet, dargestellt, um Transparenz für stattgefundene Angriffe bzw. Angriffsver-suche zu schaffen?	x ja □ nein	bei den datenschutzrelevanten Accounts
22.	Werden Passwörter nicht im Klartext gespeichert, sondern werden geeignete kryptographische Verfahren eingesetzt?	x ja □ nein	
23.	Existieren Regelungen zum automatischen Sperren von Passwörtern nach einem Sicherheitsvorfall?	x ja □ nein	Passwort-RiLi
24.	Falls Chipkarten als Mitarbeiterausweise eingesetzt werden: Eine Verwendung für Standardauthentifizierungen (z. B. Betriebs-system-Login) ist nicht möglich?	□ ja x nein	Keine Chipkarten in Verwendung
25.	Werden Standard-Authentifizierungs-Informationen (insb. Standardbenutzername und -passwort) der Softwarehersteller nach der Installation geändert?	x ja □ nein	

§ 6 Rollen-/Rechtekonzept

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*

1.	Werden Rollenprofile für die Beschäftigten erstellt, unter Einbeziehung der Einträge des Verarbeitungsverzeichnisses?	x ja □ nein	Richtlinie zum Berechtigungsmanage-ment; Verarbeitungsverzeichnis (***VV***)
2.	Wird über das Rollen-/Rechtekonzept der Zugang zu Informationen und Gebäuden/ Bereichen gezielt gesteuert und reguliert?	x ja □ nein	
3.	Existieren Regelungen zur Verwaltung der Rollen (Zuweisung, Entzug) an die Mitarbeiter?	x ja □ nein	
4.	Erfolgt regelmäßig eine Überprüfung, ob die Zuweisung der Rollen den Vorgaben entspricht und ob die Rollen noch den Anforderungen der Geschäftstätigkeit entsprechen?	x ja □ nein	Verfahren zur regelmäßigen Überprüfung VV und TOM
5.	Gibt es keine Admin-Kennungen für Nutzer, die keine administrativen Tätigkeiten ausführen?	x ja □ nein	
6.	Existieren grundsätzlich verschiedene administrative Rollen (z. B. Anlage neuer Benutzer, Durchführung von Backups, Konfiguration der Firewall) für die IT-Administration?	x ja □ nein	
7.	Wird auf Superuser-Accounts grundsätzlich verzichtet?	x ja □ nein	Es gibt nur zwei Superuser (nur GL)
8.	Wurden für Beschäftigte mit IT-Administrationsaufgaben zwei Benutzer-kennungen eingerichtet, eine Admin-Kennung und eine normale Nutzerkennung (für nicht-administrative Zwecke wie z. B. das Surfen im Internet)?	□ ja x nein	
9.	Existiert eine Regelung, die besagt, dass nicht unter Nutzung von Adminrechten im Internet gesurft oder E-Mails gelesen/versendet werden dürfen?	x ja □ nein	RiLi E-Mail und Internetnutzung

§ 7 Geräteverwaltung

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Existiert eine Geräteverwaltung, die festlegt, wer welche Geräte in welchem Bereich einsetzt?	□ ja x nein	
2.	Wird automatisch nach einer gewissen Zeitspanne der Inaktivität das Gerät gesperrt, falls manuelles Sperren bei Verlassen des	x ja □ nein	

	Einflussbereichs nicht gewährleistet werden kann?		
3.	Werden Blickschutzfolien bei potentieller unbefugter Einsichtnahme bei Monitoren und Notebookbildschirmen angebracht?	x ja □ nein	Teilweise für Mitarbeiter mit schützenswerten Daten.
4.	Ist eine Firewall aktiviert, die unerwünschte Servicedienste auf dem Endgerät blockiert?	x ja □ nein	
5.	Wird eine Anti-Viren-Lösung mit regel-mäßigen, mindestens tagesaktuellen, Signatur-Updates verwendet und existieren Regelungen, wie im Falle einer Warnmeldung zu verfahren ist?	x ja □ nein	
6.	Erfolgt eine zentrale Erfassung von Schadcode-Alarmmeldungen durch die IT-Administration?	□ ja x nein	
7.	Gibt es einen Ablaufplan der IT-Administration bei Schadcode-Befall?	x ja □ nein	
8.	Existiert ein Konzept zum Patch Management (Verwaltung von Software-Aktualisierungen), inklusive einem Update-Plan mit Übersicht der eingesetzten Software?	□ ja x nein	
9.	Wird regelmäßig eine Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software durchgeführt?	□ ja x nein	
10.	Werden Sicherheitsupdates des Betriebssystems, der installierten Software (z. B. PDF-Reader) oder von Software-bibliotheken (z. B. Java), sofern möglich, automatisch eingespielt?	x ja □ nein	
11.	Werden personenbezogene Daten auf einem Speichermedium gespeichert, das von dem Backup erfasst wird?	x ja □ nein	
12.	Ist die Einbindung von externen Geräten (beispielsweise USB-Sticks, Smartphones und externen Festplatten) auf das erforderliche Mindestmaß begrenzt?	x ja □ nein	Richtlinie, dass Speicherort immer auf
13.	Ist der Auto-Start von externen Medien (z. B. USB-Sticks) deaktiviert?	□ ja x nein	
14.	Erfolgt die Fernwartung von Endgeräten zu IT-Administrationszwecken ausschließlich über verschlüsselte Verbindungen nach	x ja □ nein	

	Authentifizierung durch den Admin und Freigabe durch den Nutzer?		
15.	Werden nur Betriebssysteme und Software eingesetzt, für die noch Sicherheitsupdates zeitnah zur Verfügung gestellt werden?	x ja □ nein	
16.	Wird die Ausführung von (aus dem Internet) heruntergeladener Software, deren Quellen als unsicher gekennzeichnet sind, verhindert?	□ ja x nein	
17.	Ist der Zugang zu Websites restriktiv verwaltet, sodass das Risiko einer Kompromittierung (z. B. durch Malware) verringert und der Zugriff auf nicht autorisierte Websites verhindert wird?	□ ja x nein	
18.	Wird die automatische Ausführung von Programmen aus dem temporären Download-Verzeichnis des Internetbrowsers verhindert?	□ ja x nein	
19.	Werden Anwendungen auf den Endgeräten möglichst ohne Adminrechte ausgeführt?	x ja □ nein	
20.	Existiert ein Prozess zur wirksamen Datenlöschung vor der Vergabe eines Endgeräts an einen anderen Mitarbeiter?	x ja □ nein	
21.	Ist ein Sicherheitskonzept für den Einsatz von Druckern, Kopierern und Multifunktions-geräten vorhanden, beispielsweise um unerlaubte Einsicht in ausgedruckte Dokumente zu verhindern und eine ordnungsgemäße Entsorgung sicherzu-stellen?	□ ja x nein	Sensible Daten bedürfen nicht des Ausdruckens.

§ 8 Mobile Speichermedien

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Erfolgt der Einsatz starker Verschlüsselung für mobile Endgeräte?	x ja □ nein	
2.	Werden Backup- und Synchronisierungs-mechanismen eingesetzt, um größeren Datenverlust bei Verlust oder Diebstahl zu verhindern?	x ja □ nein	über SaaS/Hostingdienstleister
3.	Bei Smartphones: Erfolgt der Zugang ausschließlich nach Authentifizierung (z. B. PIN, Passwort)?	x ja □ nein	

4.	Bei Smartphones: Werden biometrische Zugangsverfahren nur bei ausschließlich lokaler Speicherung der biometrischen Templates innerhalb eines Secure-Chips auf dem Smartphone und bei personen-bezogenen Daten mit keinem hohen Risiko eingesetzt?	x ja □ nein	
5.	Bei Smartphones: Wird der Einsatz von Cloud-Speichern für Datenbackup erst nach sorgfältiger Prüfung der datenschutzrechtlichen Anforderungen durchgeführt?	x ja □ nein	
6.	Bei Smartphones: Werden Mobile-Device-Management-Lösungen zur Konfiguration und Verwaltung der Geräte, der installierten Apps sowie dem Auffinden/Löschen im Verlustfall verwendet?	□ ja x nein	
7.	Bei Smartphones: Werden nur sichere Quellen für die Installation von Apps verwendet und werden Apps vorher getestet und freigegeben?	x ja □ nein	Auf Firmenhandys sind grundsätzlich nur freigegebene Apps zu installieren
8.	Wäre es ausreichend, bei Nutzung mobiler Arbeitsplätze (z. B. Notebook auf Dienstreise) auf weniger Daten als innerhalb des internen Unternehmensnetzes zugreifen zu können und wird dies in der Praxis umgesetzt?	□ ja x nein	
9.	Werden Diebstahlsicherungen für Notebooks bei Bedarf zur Verfügung gestellt?	x ja □ nein	Schließfächer an Standorten
10.	Sind Regelungen zur Privatnutzung von Notebooks und Smartphones vorhanden?	□ ja x nein	
11.	Wissen die Mitarbeiter über die Regelungen bei Verlust eines mobilen Endgerätes Bescheid?	x ja □ nein	
12.	Bei mobilen Datenträgern: Existiert eine Richtlinie zum sicheren Umgang mit mobilen Datenträgern und sind die Mitarbeiter im Umgang damit geschult?	x ja □ nein	
13.	Bei mobilen Datenträgern: Wird sichergestellt, dass die Datenträger vor und nach der Verwendung sicher gelöscht werden?	x ja □ nein	
14.	Befinden sich unbenutzte Datenträger an einem sicheren Ort?	x ja □ nein	Schließfächer

§ 9 Server

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Wird sichergestellt, dass nur kompetente bzw. geschulte Personen Administrationstätig-keiten auf den Servern durchführen dürfen?	x ja □ nein	über SaaS/Hostingdienstleister
2.	Werden verschiedene Administrationsrollen mit Rechten für unterschiedliche Administrationsaufgaben bzgl. den Servern (z. B. Updates, Konfiguration, Backup) eingesetzt?	x ja □ nein	
3.	Existiert ein geregelter Prozess zum zeitnahen Einspielen von Sicherheitsupdates der Server, wobei kritische Updates unverzüglich eingespielt werden?	x ja □ nein	über SaaS/Hostingdienstleister
4.	Erfolgt die Verwendung von eigenen Administrations-Endgeräten über eine dezidierte (=hierfür reservierte) Netzwerkverbindung?	x ja □ nein	
5.	Wird, soweit möglich, die Zwei-Faktor-Authentifizierung bei Anwendungen eingesetzt? (insbesondere bei Admin)	x ja □ nein	
6.	Sind nicht benötigte Standard-Server-Dienste (z. B. Web-server, Printserver) deaktiviert bzw. deinstalliert?	x ja □ nein	
7.	Wird der Zugriff auf serverlokale Dienste durch eine Firewall auf den Servern vor Außenzugriffen blockiert?	x ja □ nein	über SaaS/Hostingdienstleister
8.	Wurde geprüft, ob weitere Härtungsmaßnahmen für das eingesetzte Serverbetriebssystem sinnvoll sind?	x ja □ nein	über SaaS/Hostingdienstleister
9.	Ist die Versendung von Telemetriedaten (u.a. Diagnosedaten) an den Hersteller deaktiviert, sofern diese nicht als erforderlich eingeschätzt werden?	x ja □ nein	

§ 10 Webseiten und Webanwendungen

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Wird ein HTTPS-Protokoll nach dem Stand der Technik verwendet?	x ja □ nein	

2.	Sind Datenbanken auf dem Webserver mittels Firewalls abgesichert?	x ja □ nein	
3.	Erfolgt der Fernzugang zu Webservern nur mit verschlüsselter Verbindung und Zwei-Faktor-Authentifizierung?	x ja □ nein	
4.	Sind Administrationsbereiche der Weban-wendungen auf bestimmte IP-Adressen limitiert?	□ ja x nein	
5.	Dürfen nur geschulte bzw. kompetente Personen Administrationstätigkeiten auf den Servern durchführen?	x ja □ nein	
6.	Existiert ein geregelter Prozess zur Information über Sicherheitsupdates und erfolgt das zeitnahe Einspielen derselben, insbesondere bei gängigen Content-Management-Systemen (CMS)?	□ ja x nein	
7.	Wird die Durchführung von Sicherheitstests auf Webanwendungen sichergestellt?	x ja □ nein	Durch Dienstleister
8.	Wird die Übertragung personenbezogener Daten (z. B. Mail-Adresse) per HTTP-GET-Request verhindert?	□ ja x nein	
9.	Existiert eine Trennung von Webserver, Anwendungslogik und Datenhaltung einer Webanwendung durch eigene Server, die in eine Firewall-Architektur eingebunden sind?	□ ja x nein	
10.	Wird die Auffindung von Unternehmens-inhalten durch Suchmaschinen gesperrt, sofern diese Inhalte nicht durch eine Suchmaschine gefunden werden sollen?	x ja □ nein	

§ 11 Eigenes Netzwerk

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Wurde eine geeignete Netzwerksegmen-tierung durchgeführt, einschließlich der restriktiven (physischen) Trennung sensitiver Netze (z. B. medizinische Netze in Krankenhäusern oder Personalverwaltung) von Verwaltungsnetzen mithilfe von Firewall-Systemen?	x ja □ nein	über SaaS/Hostingdienstleister
2.	Wird am zentralen Internetübergang eine Firewall eingesetzt?	x ja □ nein	im Router

3.	Werden alle nicht benötigten Dienste blockiert?	x ja □ nein	
4.	Wird ein Web-Proxy eingesetzt, über den alle HTTP(S)-Verbindungen gehen müssen?	□ ja x nein	
5.	Werden HTTP(S)-Verbindungen abseits des Web-Proxy blockiert, wobei Ausnahmeregeln vermieden werden?	□ ja x nein	
6.	Erfolgt die Protokollierung und Blockierung von IOCs (= Indicators of Compromise, meist URL und IP-Hashes)?	□ ja x nein	
7.	Wird eine regelmäßige Aktualisierung der IOCs durchgeführt?	□ ja x nein	
8.	Wird eine Firewall-Architektur eingesetzt, um rein interne Systeme (z. B. Arbeitsplatz, Drucker) zu den über das Internet erreichbaren Servern (z. B. Mail-Server, Web-Server, VPN-Endpunkt) abzusichern?	x ja □ nein	Vermieterseitig
9.	Erfolgt der Einsatz von WLAN-Zugängen nur auf aktuellen WLAN-Routern mit wirksamen Zugangsmechanismen?	x ja □ nein	
10.	Bei WLAN-Gastzugang: Hat dieser keine Zugangsmöglichkeit zum internen Netzwerk?	x ja □ nein	
11.	Existiert ein geregelter Prozess zur ordnungsmäßigen Konfiguration der Firewalls und zu deren regelmäßigen Überprüfung, beispielsweise hinsichtlich der Notwendigkeit von Freigaben?	x ja □ nein	
12.	Werden Protokollierungen auf Firewall-Ebene genutzt, um auch unbefugte Zugriffe zwischen den Netzen festzustellen und zu analysieren?	□ ja x nein	
13.	Gibt es automatische Benachrichtigungen an die IT-Administration bei Verdacht auf unbefugte Verarbeitungen?	x ja □ nein	Vermieterseitig
14.	Erfolgt eine regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall?	x ja □ nein	Vermieterseitig
15.	Wird qualifiziertes Personal oder ein Dienstleister für die Konfiguration der Firewall eingesetzt?	x ja □ nein	Vermieterseitig

16.	Wird die Prüfung eingehender E-Mails mittels Anti-Malwareschutz durchgeführt?	x ja □ nein	
17.	Werden gefährliche E-Mail-Anhänge blockiert?	x ja □ nein	
18.	Wird auf die Verwendung unverschlüsselter Protokolle verzichtet?	x ja □ nein	
19.	Erfolgt der Einsatz von Intrusion-Detection-Systemen (IDS) oder Intrusion-Prevention-Systemen (IPS)?	x ja □ nein	IDS über Bitdefender
20.	Wird die Anbindung von Niederlassungen oder Homeoffice über stark verschlüsselte VPN-Verbindungen mit Client-Zertifikatsauthentifizierung durchgeführt?	x ja □ nein	

§ 12 Archivdaten

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Wurden Regelungen etabliert, welche Daten auf welcher Rechtsgrundlage aufbewahrt werden müssen und wie lange die Aufbewahrungsfrist ist?	x ja □ nein	Verarbeitungsverzeichnis und Lösch-konzept
2.	Sind die Zugänge zu den Archivdateien festgelegt und werden Zugänge dokumentiert und geprüft?	x ja □ nein	
3.	Wird sichergestellt, dass Archivdaten nach Ablauf der Aufbewahrungsfrist wirksam gelöscht werden?	x ja □ nein	Löschkonzept
4.	Erfolgt eine Archivierung auf Datenträgern, die für eine lange Speicherdauer ungeeignet sind?	□ ja x nein	
5.	Wird auf die Aufbewahrung von Archivdaten in Produktivdatenbanken verzichtet und werden stattdessen Archivdaten aus Produktiv-systemen in die Archivsysteme übertragen?	x ja □ nein	
6.	Wird die Verschlüsselung von Archivdateien mit geeignetem Schlüsselmanagement umgesetzt, bei dem die Entschlüsselungsschlüssel an mindestens zwei (örtlich) getrennten Stellen aufbewahrt werden?	x ja □ nein	

7.	Wurden geeignete Datenformate für die Archivierung von Dokumenten ausgewählt, um eine langfristige Lesbarkeit der Daten zu gewährleisten?	x ja □ nein	

§ 13 IT-Dienstleistungen

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Wird die Aufzeichnung aller Tätigkeiten von externen Dienstleistern sichergestellt?	X ja □ nein	Verarbeitungsverzeichnis, Liste Dienstleister/Auftragsverarbeiter
2.	Wird eine Verschwiegenheitsverpflichtung im Dienstleistungsvertrag aufgenommen bzw. gesondert unterzeichnet?	X ja □ nein	Im jeweiligen AVV
3.	Wurde ein interner Mitarbeiter festgelegt, der die Tätigkeiten des externen Dienstleisters überwacht (bzw. ggf. begleitet) und dokumentiert?	X ja □ nein	
4.	Existieren Regelungen zur wirksamen Datenlöschung auf Hardware (z. B. PCs, Drucker, Smartphones), die vom Dienstleister oder Hersteller zurückgenommen werden (z. B. bei Defekten, Abschreibung)?	X ja □ nein	
5.	Werden bei Einsatz von Fernwartungssoftware regelmäßig Sicherheitsupdates eingespielt und Informationen über bekannte Schwachstellen oder Fehlkonfigurationen beachtet?	□ ja x nein	
6.	Wird die Fernwartung externer Dienstleister protokolliert und wird der Zugang nur auf das zu wartende System begrenzt? Wenn möglich, wird dies durch einen Mitarbeiter am Bildschirm des gewarteten Systems digital nachverfolgt?	□ ja x nein	Es gibt keine externen Dienstleister

§ 14 Protokollierungen

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Wurde ein Konzept zur Protokollierung von Benutzeraktivitäten, technischen Systemer-eignissen, Fehlerzuständen und Internet-aktivitäten erstellt und dabei datenschutz-rechtliche Anforderungen berücksichtigt?	□ ja x nein	

2.	Erfolgt die Speicherung von Log-Dateien auf einem eigenen Log-Server?	X ja □ nein	
3.	Wurden die Uhren der verwendeten Informationsverarbeitungssysteme (PCs, Notebooks, etc.) mit geeigneten Zeitquellen synchronisiert, um eine gezielte Analyse bei Sicherheitsereignissen zu ermöglichen?	□ ja x nein	Werkseinstellungen/Abgleich mit offiziellen Zeiten im Internet
4.	Wird die Einhaltung der Zweckbindung der Log-Dateien sichergestellt?	x ja □ nein	
5.	Finden regelmäßige anlasslose Auswertungen der Log-Dateien zur Erkennung von ungewöhnlichen Einträgen statt?	□ ja x nein	

§ 15 Back-ups

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Gibt es einen Notfallplan zur Business Continuity, der Regelungen enthält, welche Systeme in welcher Reihenfolge wieder instandgesetzt werden, welche (externen) Personen/ Dienstleister im Notfall zu Rate gezogen werden können und welche Meldeverpflichtungen es gibt?	x ja □ nein	Notfallplan
2.	Wird der Notfallplan regelmäßig überprüft?	x ja □ nein	
3.	Existiert ein schriftlich fixiertes Backup-Konzept?	□ ja x nein	Über SaaS/Hostingdienstleister werden Backups gesichert
4.	Werden Backups nach der 3-2-1 Regel durchgeführt, d.h. 3 Datenspeicherungen, 2 verschiedene Backup Medien (auch „Offline“ wie Bandsicherungen) und 1 davon an einem externen Standort?	□ ja x nein	Es wird ein 3-2 Backup gesichert
5.	Gibt es eine geeignete physische Aufbe-wahrung von Backup Medien?	x ja □ nein	Über SaaS/Hostingdienstleister
6.	Wird regelmäßig überprüft, ob mindestens ein Backup täglich durchgeführt wird?	□ ja x nein	Über SaaS/Hostingdienstleister wird täglich gesichert, jedoch nicht täglich geprüft
7.	Finden regelmäßige Tests statt, um sicherzustellen, dass alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert?	□ ja x nein	Über SaaS/Hostingdienstleister

8.	Ist mindestens ein Backup-System durch Schadcode nicht verschlüsselbar?	x ja □ nein	Über SaaS/Hostingdienstleister
9.	Wird weitgehend auf Makros in Office-Dokumenten im Betriebsalltag verzichtet, um vor Ransomware zu schützen?	x ja □ nein	
10.	Erlaubt das System ausschließlich signierte Microsoft Office-Makros oder werden die Beschäftigten regelmäßig, beispielsweise einmal pro Jahr, über Risiken einer Makro-Aktivierung informiert?	□ ja x nein	Es werden keine Makros eingesetzt
11.	Wird die automatische Ausführung von heruntergeladenen Programmen verhindert?	□ ja x nein	
12.	Ist der Windows Script Host (WSH) auf Endgeräten deaktiviert (sofern nicht zwingend benötigt)?	□ ja x nein	
13.	Wurde geprüft, ob die Einschränkung von Powershell-Skripten mit dem „Constrained-Language Mode“ auf Windows-Endgeräten möglich und sinnvoll durchführbar ist?	□ ja x nein	
14.	Wird ein Web-Proxy mit (tages-)aktuellen Sperrlisten von Schadcode-Download-Seiten genutzt?	□ ja x nein	
15.	Enthält der Notfallplan den Umgang mit Verschlüsselungstrojanern und liegt dieser Plan auch in Papierform vor?	□ ja x nein	
16.	Wird die Backup- und Recovery-Strategie überprüft, um sicherzustellen, dass Backups durch Ransomware nicht verschlüsselt werden können?	□ ja x nein	

§ 16 Verschlüsselung

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Sind klare Regeln für die effektive Nutzung von Kryptographie, einschließlich der Schlüsselverwaltung, definiert?	x ja □ nein	
2.	Wird mit Hash-Verfahren nach dem Stand der Technik die Integrität von Daten, Software und IT-Systemen sichergestellt?	x ja □ nein	
3.	Erfolgt die Passwortspeicherung nur dann mit „normalen“ Hashfunktionen (z. B. SHA-Klasse), wenn das Passwort	□ ja x nein	

	mindestens 12 Stellen lang ist? Und werden dabei Salt-Werte eingesetzt, um vor Einträgen in Datenbanken (Rainbow Tables) zu schützen?		
4.	Erfolgt die Passwortspeicherung mit Salt nach dem Stand der Technik?	x ja □ nein	PBkDF2
5.	Erfolgt die symmetrische Verschlüsselung nach dem Stand der Technik?	x ja □ nein	
6.	Erfolgt die asymmetrische Verschlüsselung nach dem Stand der Technik?	x ja □ nein	
7.	Besteht eine wirksame Schlüsselverwaltung (Generierung, Ausgabe, Sperrung) beim Einsatz kryptographischer Verfahren und wird diese überprüft?	x ja □ nein	
8.	Werden geheime Schlüssel durch starke Passwörter mit mindestens 16 Stellen geschützt? Und wird bei hohem Risiko der Einsatz von HSM (Hardware Security Modulen) geprüft?	□ ja x nein	Keine HSM Nutzung
9.	Werden SSL-Zertifikate ausschließlich von vertrauenswürdigen Zertifizierungsstellen beschafft?	x ja □ nein	
10.	Erfolgt die Verwendung von HTTPS nach dem Stand der Technik und wird dies überprüft?	x ja □ nein	
11.	Werden keine kryptographischen Verfahren mit bekannten Schwachstellen oder zu kurzer Schlüssellänge mehr verwendet? Falls Altsysteme diese noch erfordern: Wird dies regelmäßig überprüft und wurde eine individuelle Risikoanalyse durchgeführt?	□ ja x nein	

§ 17 Datentransfer

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Bestehen klare Regeln für alle Arten von internen Datentransfers sowie von externen Datentransfers nach außen?	x ja □ nein	Möglichst Verarbeitung nur in der EU, ansonsten nur unter den Voraussetzungen der Art. 44 ff. DSGVO
2.	Sind Verfahren zur Nutzung von Cloud-Diensten, einschließlich einer möglichen Ausstiegsstrategie, etabliert?	x ja □ nein	

3.	Werden mobile Datenträger wie DVD, USB-Sticks und Festplatten gemäß dem aktuellen Stand der Technik verschlüsselt?	□ ja x nein	Wird nicht genutzt
4.	Wird bei E-Mails und Cloud-Plattformen die Transportverschlüsselung von personenbezogenen Daten nach dem Stand der Technik bei normalem Risiko gewährleistet?	x ja □ nein	
5.	Wird bei E-Mails und Cloud-Plattformen die Transport- und Inhaltsverschlüsselung von personenbezogenen Daten nach dem Stand der Technik bei hohem Risiko sichergestellt?	x ja □ nein	
6.	Werden bei Messenger-Diensten die Transport- und Inhaltsverschlüsselung der Nachrichten und Dateien gewährleistet?	x ja □ nein	
7.	Wird die Integrität von personenbezogenen Daten durch digitale Signaturen zumindest bei hohem Risiko sichergestellt?	□ ja x nein	
8.	Wird bei HTTPS der Einsatz von Client-Zertifikaten zum Nachweis der Authentizität bei geschlossenem Nutzerkreis berücksichtigt?	x ja □ nein	
9.	Wird die verschlüsselte Nutzung von DNS-Diensten (DNSSec, DNS-over-TLS) geprüft?	□ ja x nein	

§ 18 Software

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Sind relevante Mitarbeiter darüber geschult, dass Security-by-Design (Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität) als Teilmenge von Data-Protection-By-Design eine gesetzliche Datenschutzanforderung ist und Einfluss auf zentrale Designentscheidungen hat?	x ja □ nein	Richtlinie Privacy by Design & Default
2.	Findet eine Trennung von Produktivsystem zu Entwicklungs-/Testsystem statt?	x ja □ nein	
3.	Ist der Zugang zum Source-Code bei der Entwicklung von Software beschränkt?	x ja □ nein	
4.	Werden keine personenbezogenen Daten oder Zugangsdaten in der Source-Code-Verwaltung abgelegt?	x ja □ nein	

5.	Werden System- und Sicherheitstests durchgeführt?	x ja □ nein	
6.	Werden ausreichende Testzyklen berück-sichtigt?	x ja □ nein	
7.	Erfolgt ein fortlaufendes Inventarisieren der Versionen von Software oder Komponenten (z.B. Frameworks, Bibliotheken) sowie deren Abhängigkeiten?	x ja □ nein	
8.	Werden Standardsoftware und ent-sprechende Updates nur aus vertrauens-würdigen Quellen bezogen?	x ja □ nein	
9.	Ist sichergestellt, dass ein fortlaufender Plan zur Überwachung, Bewertung und Anwen-dung von Updates oder Konfigurations-änderungen für die gesamte Lebenszeit einer Softwareanwendung besteht?	x ja □ nein	

§ 19 Auftragsverarbeiter

Nr.	*Frage*	*Antwort*	*Erläuterung der Antwort*
1.	Werden nur Dienstleister verwendet, die Garantien in Form von Dokumenten zur Verfügung stellen können?	x ja □ nein	gemäß jeweiligen AVV
2.	Sind die Sicherheitsmaßnahmen nach Art. 32 DSGVO als Bestandteil eines Auftragsverarbeitungsvertrags an die Dienstleistung angepasst?	x ja □ nein	gemäß jeweiligen AVV
3.	Kann die Wirksamkeit der Garantien durch geeignete Zertifizierungen (ansatzweise) nachgewiesen werden?	x ja □ nein	gemäß jeweiligen AVV
4.	Werden Vor-Ort-Kontrollen durch den Verantwortlichen nicht ausgeschlossen?	x ja □ nein	gemäß jeweiligen AVV
5.	Dürfen Auftragsverarbeiter keine weiteren Subdienstleister ohne Information des Auftraggebers aufnehmen, wobei dieser dann mindestens ein Widerspruchsrecht hat?	x ja □ nein	gemäß jeweiligen AVV
6.	Verfügen die Auftragsverarbeiter über Prozesse bei der Erkennung von Datenschutzverletzungen und melden sie diese unverzüglich dem Verantwortlichen?	x ja □ nein	gemäß jeweiligen AVV

7.	Werden Transfers in unsichere Drittländer ggf. nur mit weiteren technischen Schutzmaß-nahmen durchgeführt?	x ja □ nein	gemäß jeweiligen AVV
8.	Werden Daten bei der Auftragsverarbeitung spätestens nach Vertragsende wirksam gelöscht?	x ja □ nein	gemäß jeweiligen AVV
9.	Können Angaben zur Löschmethodik bei Bedarf zur Verfügung gestellt werden?	x ja □ nein	gemäß jeweiligen AVV
10.	Erfolgt eine regelmäßige Überprüfung der Auftragsverarbeiter hinsichtlich Sicherheits-praktiken und Dienstleistungserbringung?	x ja □ nein	gemäß jeweiligen AVV