Technische und organisatorische Maßnahmen
der GrantLift GmbH
(Stand: 01/2026)

§ 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 DSGVO (***Verletzung der Sicherheit***) bekannt?	x ja □ nein	Richtlinie Vorgehen bei Datenschutz-verletzungen

11.	Existieren Eskalationsprozesse bei Sicherheitsverletzungen, inklusive der klaren Information darüber, wer wann wie zu informieren ist, insbesondere im Notfallmanagement?	x ja □ nein	Notfallplan
12.	Werden Sicherheitsvorkommnissen konsequent dokumentiert (***Security Reporting***)?	x ja □ nein	Beim Unternehmen und DSB
13.	Wird die Zusammenarbeit zwischen dem DSB und dem ISB aktiv durch die Unternehmensleitung 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 Gebäudesicherung 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) vorhanden, 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	x ja □ nein	

	verschlüsselten E-Mail-Anhängen (z. B. Zip-Datei mit Passwort)?		
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 Berechtigungsmanagement; 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 datenschutzkonforme 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. Angriffsversuche 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. Betriebssystem-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 Berechtigungsmanagement; 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 Einflussbereichs nicht gewährleistet werden kann?	x ja □ nein	
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 Authentifizierung durch den Admin und Freigabe durch den Nutzer?	x ja □ nein	
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 Multifunktionsgeräten vorhanden, beispielsweise um unerlaubte Einsicht in ausgedruckte Dokumente zu verhindern und eine ordnungsgemäße Entsorgung sicherzustellen?	□ 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 Synchronisierungsmechanismen 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 personenbezogenen 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?	□ ja x nein	Auf Firmenhandys wird die Nutzung auf ausschließlich notwendige Apps nahegelegt
8.	Wäre es ausreichend, bei Nutzung mobiler Arbeitsplätze (z. B. Notebook auf Dienstreise)	□ ja x nein	

	auf weniger Daten als innerhalb des internen Unternehmensnetzes zugreifen zu können und wird dies in der Praxis umgesetzt?		
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?	□ ja x nein	wird eingeführt
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 Administrationstätigkeiten 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	□ ja x nein	

	Webanwendung durch eigene Server, die in eine Firewall-Architektur eingebunden sind?		
10.	Wird die Auffindung von Unternehmensinhalten 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 Netzwerksegmentierung 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	x ja □ nein	

	und zu deren regelmäßigen Überprüfung, beispielsweise hinsichtlich der Notwendigkeit von Freigaben?		
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 Systemereignissen, Fehlerzuständen und Internetaktivitäten erstellt und dabei datenschutzrechtliche 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 Aufbewahrung 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 mindestens 12 Stellen lang ist? Und werden dabei Salt-Werte eingesetzt, um vor Einträgen in Datenbanken (Rainbow Tables) zu schützen?	□ ja x nein	
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 wirksame Transfermechanismen
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 berücksichtigt?	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 entsprechende Updates nur aus vertrauenswürdigen Quellen bezogen?	x ja □ nein	
9.	Ist sichergestellt, dass ein fortlaufender Plan zur Überwachung, Bewertung und Anwendung von Updates oder Konfigurationsänderungen 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 Schutzmaßnahmen 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

Technical and Organisational Measures

GrantLift GmbH
(As of: 01/2026)

1. General Information

This document is part of the data protection documentation of the data protection management system. This version of the document supersedes all earlier versions and editions.

2. General Organisational Structure

No.	Question	Answer	Explanation of Answer
1	Is information security considered in all processes?	x yes □ no	Privacy by Design & Default guidelines
2	Are security policies and guidelines defined, approved by management, and communicated to staff?	x yes □ no	Guideline on information security and on data protection
3	Are regular reviews of the effectiveness of technical and organisational measures carried out?	x yes □ no	Procedure for regular review of the processing register (RoPA) and TOMs
4	Are concepts and documentation in the security environment regularly reviewed and kept up to date?	x yes □ no	Together with the Data Protection Officer (DPO)
5	Is a suitable Information Security Management System (ISMS) used depending on company size?	□ yes x no	Not currently (small company)
6	Are roles and responsibilities in the area of security known and filled within the organisation, including the Information Security Officer (ISO), IT manager and DPO?	x yes □ no	ISO = Gabriel Kienberger
7	Is the DPO consistently involved in security matters?	x yes □ no	
8	Does the DPO have sufficient technical qualification for security-related issues, with the opportunity for further training in this area?	x yes □ no	DPO is a specialist lawyer for information technology law with a continuing education obligation
9	Are regular audits by the DPO conducted pursuant to Art. 32 GDPR on the security of processing?	x yes □ no	
10	Is the competent data protection supervisory authority and the reporting obligations under Art. 33 and 34 GDPR (security breaches) known?	x yes □ no	Guideline: Procedure for Data Protection Breaches
11	Do escalation processes exist for security breaches, including clear information on who is to be informed, when, and how, especially in emergency management?	x yes □ no	Emergency plan
12	Are security incidents consistently documented (Security Reporting)?	x yes □ no	At the company and with the DPO
13	Is cooperation between the DPO and the ISO actively supported by company management?	x yes □ no	
14	Is intelligence on (new) digital threats gathered and are potential impacts on the organisation derived?	x yes □ no	Bitdefender – malware detection

3. Protection of Infrastructure Against Unauthorised Access and Natural Events

No.	Question	Answer	Explanation of Answer
1	Is there an overall concept for building security in general, including fire protection, access restrictions, and access control?	x yes □ no	By the landlord
2	Does a concept for access regulations and physical access control exist?	x yes □ no	By the landlord
3	Are there clear rules for dealing with visitors as part of the concept, including escort, security zones, visitor badges, logging, and a designated employee for visitors?	x yes □ no	Escorted visits only
4	Are rules in place for dealing with external service providers (e.g. contract work, tradespeople, system maintenance) such as confidentiality agreements, personal escort in security zones, or logging?	x yes □ no	Escorted service providers only
5	Have different security zones been established?	x yes □ no	Visitor area is separate
6	Is there a current overview of access rights management in security zones (which employee may access which zone)?	x yes □ no	For visitors only
7	Is access to security zones restricted by appropriate technology?	□ yes x no	
8	Are self-closing doors used at zone transitions in security areas?	□ yes x no	
9	Are secure locking systems with documented key management implemented?	x yes □ no	By the landlord
10	Is there a fire protection concept?	x yes □ no	By the landlord
11	Are fire/smoke detection systems used as part of the fire protection concept?	x yes □ no	By the landlord
12	Are automatic extinguishing systems used in server rooms?	□ yes x no	
13	Are fire-resistant cabinets/safes used for storing essential components (e.g. backup tapes, important original documents)?	□ yes x no	
14	Are buildings (e.g. walls, windows) and infrastructure (e.g. cables, hazard detection systems) regularly inspected and maintained?	x yes □ no	By the landlord
15	If business premises exist: Is the premises fenced?	□ yes x no	No premises/outdoor area
16	Are there sturdy, break-in-resistant windows and doors on the ground floor?	□ yes x no	4th floor
17	Are alarm systems used for burglary detection, especially outside working hours?	x yes □ no	By the landlord
18	Is security personnel (if applicable, external) deployed?	x yes □ no	By the landlord
19	Is video surveillance used in compliance with data protection requirements, especially for monitoring access protection?	□ yes x no	
20	Is adequate air conditioning of server rooms ensured?	□ yes x no	No own servers
21	Are there no (openable) windows in server rooms?	□ yes x no	
22	Is an uninterruptible power supply (UPS) used for server systems (in case of short power outages or fluctuations)?	□ yes x no	
23	Are measures taken against elemental hazards (in particular fire, smoke, vibrations, chemical reactions, flooding, power outages, explosions, attacks/vandalism)?	□ yes X no	

24	Have risks from flooding/heavy rain been assessed, especially for server rooms in basements or other at-risk areas?	□ yes x no	

4. Employee Training

No.	Question	Answer	Explanation of Answer
1	Does all personnel receive training on information security and data protection, to the extent relevant to their respective function?	x yes □ no	Training via DPO
2	Are data protection trainings conducted for new employees promptly after commencement of the employment relationship?	x yes □ no	See above
3	Are regular refresher trainings carried out for existing staff, e.g. once per year?	x yes □ no	See above
4	Do all persons in the company regularly receive information about news on data protection and IT security?	x yes □ no	E.g. via email, Slack
5	Are relevant policies, such as those on email/internet use, handling of malware alerts, and use of encryption technologies, kept up to date and easy to find?	x yes □ no	Security Guideline on Email and Internet Use, AI Policy, Password Policy, etc.
6	Are the presentations with training content accessible to all affected employees?	x yes □ no	
7	Are selected employees involved in detecting security breaches aware of internal incident management processes, including reporting under Art. 33 GDPR and the emergency plan?	x yes □ no	Guideline: Procedure for Data Protection Breaches, Emergency Plan
8	Do training contents address how cyber attacks are initiated via social engineering?	x yes □ no	
9	Are employees made aware in training of the risks of email communication, especially with encrypted attachments (e.g. zip files with password)?	x yes □ no	
10	Are employees trained in training content to recognise fraudulent emails, e.g. by checking sender addresses, anomalies, and embedded links?	x yes □ no	
11	Are employees who interact with external parties such as suppliers sensitised regarding policies, processes, and conduct, including which data may be shared in what form and what may be security-critical?	x yes □ no	
12	Are employees affected by remote work instructed on the secure use of home office solutions and are specific risks highlighted?	x yes □ no	Mobile Office Guideline

5. Authentication

No.	Question	Answer	Explanation of Answer
1	Is all personnel instructed in the use of authentication methods and mechanisms?	x yes □ no	
2	Is there a regulated process for the central management of user identities, including creation (e.g. new employees), modification (e.g. name change after marriage), and deletion (e.g. departure of employee)?	x yes □ no	Authorisation Management Guideline; Security Guideline for IT Administrators
3	Are unique identifiers assigned to each user and are group identifiers avoided?	x yes □ no	Generally yes; student workers are assigned to an existing licence

4	If group identifiers are mandatorily used: Is GDPR-compliant logging of associated user activities in place?	x yes □ no	Generally yes; student workers are assigned to an existing licence
5	Is the use of strong passwords promoted and a policy published for it?	x yes □ no	Password Policy
6	Is the password policy for strong passwords automatically enforced in systems with user accounts?	x yes □ no	Via Password Policy
7	Is the selection of weak passwords prevented in applications?	x yes □ no	Via Password Policy
8	Is there a requirement that passwords be changed after defined periods (e.g. 60 days)?	□ yes x no	Password change only upon suspicion of potential third-party access or possible loss of credentials; cf. Password Policy
9	Are passwords blocked after a security incident (even on suspicion) and must be reset by the user?	x yes □ no	
10	Is a password change required at the first login of a new user or when a password is reset by IT (e.g. after forgetting the password)?	x yes □ no	
11	Are employees prohibited from sharing passwords (including with colleagues, supervisors, or the IT department), and in exceptional cases (e.g. extended illness) is the password reset by IT and this action documented?	x yes □ no	Via Password Policy
12	Have employees been informed that passwords must not be written on notes or notice boards?	x yes □ no	Via Password Policy
13	Is storage of passwords in the browser without protection by a master password avoided?	x yes □ no	
14	Is reuse of a password for different services avoided, provided no central identity management (e.g. Active Directory) is used?	x yes □ no	Password manager should always be used
15	Is transmission of passwords by email (e.g. for a company account to a cloud service) prevented?	x yes □ no	
16	Are particularly strong passwords used for local admin accounts?	x yes □ no	
17	Is two- or multi-factor authentication used?	x yes □ no	
18	Is two-factor authentication consistently used for admin accounts?	x yes □ no	For data protection-relevant accounts
19	Is automatic locking of accounts implemented after too many failed login attempts using the wrong password (either time-based or complete lockout requiring IT contact)?	x yes □ no	For data protection-relevant accounts
20	Is there a time delay between individual login attempts (especially for internet-accessible applications) to hinder automated online attacks?	x yes □ no	For data protection-relevant accounts
21	Is the number of failed logins displayed to a user who successfully logs in, to provide transparency regarding attacks or attack attempts?	x yes □ no	For data protection-relevant accounts
22	Are passwords not stored in plain text, but instead appropriate cryptographic methods used?	x yes □ no	
23	Are rules in place for the automatic locking of passwords after a security incident?	x yes □ no	Password Policy
24	If chip cards are used as employee ID cards: Is use for standard authentication (e.g. operating system login) not possible?	□ yes x no	No chip cards in use

25	Are default authentication credentials (in particular default username and password) from software manufacturers changed after installation?	x yes □ no	

6. Role and Rights Concept

No.	Question	Answer	Explanation of Answer
1	Are role profiles created for employees, incorporating entries from the Record of Processing Activities (RoPA)?	x yes □ no	Authorisation Management Guideline; Record of Processing Activities (RoPA)
2	Is access to information and buildings/areas specifically controlled and regulated through the role/rights concept?	x yes □ no	
3	Are rules in place for managing roles (assignment, revocation) for employees?	x yes □ no	
4	Is there a regular review of whether the role assignments comply with requirements and whether the roles still meet the needs of the business?	x yes □ no	Procedure for regular review of RoPA and TOMs
5	Are there no admin accounts for users who do not carry out administrative tasks?	x yes □ no	
6	Do different administrative roles generally exist (e.g. creating new users, performing backups, configuring the firewall) for IT administration?	x yes □ no	
7	Is the use of superuser accounts generally avoided?	x yes □ no	Only two superusers exist (management only)
8	Have employees with IT administration tasks been set up with two user accounts, one admin account and one regular user account (for non-administrative purposes such as internet browsing)?	□ yes x no	
9	Is there a rule stating that browsing the internet or reading/sending emails must not be done using admin rights?	x yes □ no	Email and Internet Use Guideline

7. Device Management

No.	Question	Answer	Explanation of Answer
1	Is there a device management system that determines who uses which devices in which area?	□ yes x no	
2	Is the device automatically locked after a period of inactivity, in cases where manual locking upon leaving the area of influence cannot be ensured?	x yes □ no	
3	Are privacy filters applied to monitors and laptop screens where unauthorised viewing is possible?	x yes □ no	Partially for employees handling sensitive data
4	Is a firewall activated that blocks unwanted service connections on the endpoint device?	x yes □ no	
5	Is an anti-virus solution used with regular, at least daily, signature updates, and are rules in place for how to proceed in case of a warning?	x yes □ no	
6	Is centralised recording of malware alerts conducted by IT administration?	□ yes x no	
7	Is there a response plan for IT administration in the event of a malware infection?	x yes □ no	
8	Is there a patch management concept (management of software updates), including an update plan with an overview of the software in use?	□ yes x no	

9	Is a regular evaluation of information on security vulnerabilities in the software in use carried out?	□ yes x no	
10	Are security updates for the operating system, installed software (e.g. PDF reader), or software libraries (e.g. Java), where possible, applied automatically?	x yes □ no	
11	Are personal data stored on a storage medium that is covered by the backup process?	x yes □ no	
12	Is the use of external devices (e.g. USB sticks, smartphones, and external hard drives) limited to the required minimum?	x yes □ no	Policy requiring storage location to always be on the server
13	Is auto-start of external media (e.g. USB sticks) disabled?	□ yes x no	
14	Is remote maintenance of endpoints for IT administration purposes carried out exclusively via encrypted connections after authentication by the admin and approval by the user?	x yes □ no	
15	Are only operating systems and software used for which security updates are promptly available?	x yes □ no	
16	Is execution of software downloaded from the internet, whose sources are flagged as unsafe, prevented?	□ yes x no	
17	Is access to websites restrictively managed to reduce the risk of compromise (e.g. through malware) and prevent access to unauthorised websites?	□ yes x no	
18	Is automatic execution of programs from the temporary download directory of the internet browser prevented?	□ yes x no	
19	Are applications on endpoint devices run without admin rights where possible?	x yes □ no	
20	Is there a process for effective data deletion before reassigning an endpoint device to another employee?	x yes □ no	
21	Is there a security concept for the use of printers, copiers, and multifunction devices, for example to prevent unauthorised viewing of printed documents and to ensure proper disposal?	□ yes x no	Sensitive data does not need to be printed

8. Mobile Storage Media

No.	Question	Answer	Explanation of Answer
1	Is strong encryption used for mobile devices?	x yes □ no	
2	Are backup and synchronisation mechanisms used to prevent major data loss in case of loss or theft?	x yes □ no	Via SaaS/hosting service providers
3	For smartphones: Is access only granted after authentication (e.g. PIN, password)?	x yes □ no	
4	For smartphones: Are biometric access methods only used where biometric templates are stored exclusively locally within a secure chip on the smartphone and for personal data with no high risk?	x yes □ no	
5	For smartphones: Is the use of cloud storage for data backup carried out only after careful review of data protection requirements?	x yes □ no	
6	For smartphones: Are Mobile Device Management (MDM) solutions used for configuring and managing devices, installed	□ yes x no	

	apps, and for locating/wiping in the event of loss?		
7	For smartphones: Are only secure sources used for installing apps, and are apps tested and approved beforehand?	□ yes x no	On company phones, use is limited to necessary apps only
8	Would it be sufficient, when using mobile workplaces (e.g. laptop on a business trip), to access fewer data than within the internal company network, and is this implemented in practice?	□ yes x no	
9	Are anti-theft devices for laptops provided as needed?	x yes □ no	Lockers at locations
10	Are rules on private use of laptops and smartphones in place?	□ yes x no	
11	Are employees aware of the rules regarding loss of a mobile device?	x yes □ no	
12	For mobile data carriers: Is there a policy on the safe handling of mobile data carriers, and are employees trained in this?	□ yes x no	Being introduced
13	For mobile data carriers: Is it ensured that data carriers are securely erased before and after use?	x yes □ no	
14	Are unused data carriers kept in a secure location?	x yes □ no	Lockers

9. Servers

No.	Question	Answer	Explanation of Answer
1	Is it ensured that only competent or trained persons are permitted to carry out administration tasks on the servers?	x yes □ no	Via SaaS/hosting service providers
2	Are different administration roles with rights for different administration tasks on the servers (e.g. updates, configuration, backup) used?	x yes □ no	
3	Is there a regulated process for the timely application of security updates to servers, with critical updates applied without delay?	x yes □ no	Via SaaS/hosting service providers
4	Are dedicated administration endpoints used via a dedicated (reserved) network connection?	x yes □ no	
5	Is two-factor authentication used in applications where possible (especially for admin access)?	x yes □ no	
6	Are unneeded default server services (e.g. web server, print server) disabled or uninstalled?	x yes □ no	
7	Is access to server-local services blocked by a firewall on the servers against external access?	x yes □ no	Via SaaS/hosting service providers
8	Has it been reviewed whether further hardening measures for the server operating system in use are appropriate?	x yes □ no	Via SaaS/hosting service providers
9	Is the transmission of telemetry data (including diagnostic data) to the manufacturer disabled, if not deemed necessary?	x yes □ no	

10. Websites and Web Applications

No.	Question	Answer	Explanation of Answer
1	Is HTTPS used in accordance with the current state of the art?	x yes □ no	
2	Are databases on the web server secured by firewalls?	x yes □ no	
3	Is remote access to web servers only carried out via encrypted connections and two-factor authentication?	x yes □ no	

4	Are administration areas of web applications limited to specific IP addresses?	□ yes x no	
5	Are only trained or competent persons permitted to carry out administration tasks on servers?	x yes □ no	
6	Is there a regulated process for being informed about security updates and for their timely application, especially for common Content Management Systems (CMS)?	□ yes x no	
7	Is security testing of web applications ensured?	x yes □ no	By service provider
8	Is the transmission of personal data (e.g. email address) via HTTP GET requests prevented?	□ yes x no	
9	Is there a separation of web server, application logic, and data storage within its own servers integrated into a firewall architecture?	□ yes x no	
10	Is indexing of company content by search engines blocked where such content should not be found by a search engine?	x yes □ no	

11. Own Network

No.	Question	Answer	Explanation of Answer
1	Has appropriate network segmentation been carried out, including the restrictive (physical) separation of sensitive networks (e.g. medical networks in hospitals or HR management) from administrative networks using firewall systems?	x yes □ no	Via SaaS/hosting service providers
2	Is a firewall used at the central internet gateway?	x yes □ no	In the router
3	Are all unneeded services blocked?	x yes □ no	
4	Is a web proxy used through which all HTTP(S) connections must pass?	□ yes x no	
5	Are HTTP(S) connections outside the web proxy blocked, avoiding exception rules?	□ yes x no	
6	Are IOCs (Indicators of Compromise, mainly URL and IP hashes) logged and blocked?	□ yes x no	
7	Are IOCs regularly updated?	□ yes x no	
8	Is a firewall architecture used to secure purely internal systems (e.g. workstation, printer) from internet-accessible servers (e.g. mail server, web server, VPN endpoint)?	x yes □ no	By landlord
9	Are WLAN access points used only on current WLAN routers with effective access mechanisms?	x yes □ no	
10	For WLAN guest access: Does this have no access to the internal network?	x yes □ no	
11	Is there a regulated process for the proper configuration of firewalls and their regular review, e.g. regarding the necessity of releases?	x yes □ no	
12	Is logging at firewall level used to detect and analyse unauthorised access between networks?	□ yes x no	
13	Are automatic notifications to IT administration generated upon suspicion of unauthorised processing?	x yes □ no	By landlord
14	Is the proper configuration of the firewall regularly reviewed?	x yes □ no	By landlord
15	Is qualified personnel or a service provider used for configuring the firewall?	x yes □ no	By landlord

16	Is incoming email checked by anti-malware protection?	x yes □ no	
17	Are dangerous email attachments blocked?	x yes □ no	
18	Is the use of unencrypted protocols avoided?	x yes □ no	
19	Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used?	x yes □ no	IDS via Bitdefender
20	Are branches or home office connections made via strongly encrypted VPN connections with client certificate authentication?	x yes □ no	

12. Archive Data

No.	Question	Answer	Explanation of Answer
1	Have rules been established regarding which data must be retained on which legal basis and what the retention period is?	x yes □ no	Record of Processing Activities (RoPA) and Deletion Concept
2	Are access rights to archive files defined, and is access documented and reviewed?	x yes □ no	
3	Is it ensured that archive data is effectively deleted upon expiry of the retention period?	x yes □ no	Deletion Concept
4	Is archiving carried out on data carriers unsuitable for long-term storage?	□ yes x no	
5	Is storage of archive data in production databases avoided, and is archive data transferred from production systems to archive systems instead?	x yes □ no	
6	Is encryption of archive files implemented with appropriate key management, where decryption keys are stored at at least two (geographically) separate locations?	x yes □ no	
7	Have appropriate data formats been selected for archiving documents to ensure long-term readability of the data?	x yes □ no	

13. IT Services

No.	Question	Answer	Explanation of Answer
1	Is the recording of all activities of external service providers ensured?	X yes □ no	Record of Processing Activities, List of Service Providers/Processors
2	Is a confidentiality obligation included in the service contract or signed separately?	X yes □ no	In the respective DPA
3	Has an internal employee been designated to monitor (and if applicable escort) and document the activities of the external service provider?	X yes □ no	
4	Are rules in place for effective data deletion on hardware (e.g. PCs, printers, smartphones) that is returned by the service provider or manufacturer (e.g. in case of defects, write-offs)?	X yes □ no	
5	When remote maintenance software is used: Are security updates regularly applied and information about known vulnerabilities or misconfigurations taken into account?	□ yes x no	
6	Is remote maintenance by external service providers logged, and is access limited to the system being maintained? Where possible, is this monitored digitally by an employee on screen?	□ yes x no	No external service providers

14. Logging

No.	Question	Answer	Explanation of Answer
1	Has a concept for logging user activities, technical system events, error states, and internet activities been established, while taking into account data protection requirements?	□ yes x no	
2	Are log files stored on a dedicated log server?	X yes □ no	
3	Have the clocks of the information processing systems in use (PCs, laptops, etc.) been synchronised with appropriate time sources to enable targeted analysis during security events?	□ yes x no	Factory settings / synchronisation with official internet time sources
4	Is compliance with the purpose limitation of log files ensured?	x yes □ no	
5	Are regular unprompted evaluations of log files carried out to detect unusual entries?	□ yes x no	

15. Backups

No.	Question	Answer	Explanation of Answer
1	Is there an emergency/business continuity plan that includes rules on which systems are to be restored in which order, which (external) persons/service providers can be consulted in an emergency, and what reporting obligations exist?	x yes □ no	Emergency Plan
2	Is the emergency plan regularly reviewed?	x yes □ no	
3	Does a written backup concept exist?	□ yes x no	Backups are secured via SaaS/hosting service providers
4	Are backups performed according to the 3-2-1 rule, i.e. 3 copies of data, 2 different backup media (including 'offline' such as tape backups), and 1 at an external location?	□ yes x no	A 3-2 backup is performed
5	Is there appropriate physical storage of backup media?	x yes □ no	Via SaaS/hosting service providers
6	Is it regularly verified that at least one backup is performed daily?	□ yes x no	Daily backup via SaaS/hosting service providers, but not checked daily
7	Are regular tests conducted to ensure that all relevant data is included in the backup process and that restoration works?	□ yes x no	Via SaaS/hosting service providers
8	Is at least one backup system protected against encryption by malware?	x yes □ no	Via SaaS/hosting service providers
9	Is the use of macros in Office documents largely avoided in day-to-day operations to protect against ransomware?	x yes □ no	
10	Does the system allow only signed Microsoft Office macros, or are employees regularly (e.g. once per year) informed about the risks of enabling macros?	□ yes x no	No macros are used
11	Is automatic execution of downloaded programs prevented?	□ yes x no	
12	Is the Windows Script Host (WSH) disabled on endpoints (unless absolutely necessary)?	□ yes x no	
13	Has it been examined whether restricting PowerShell scripts using 'Constrained Language Mode' on Windows endpoints is feasible and sensible?	□ yes x no	
14	Is a web proxy with up-to-date (daily) blocklists of malware download sites used?	□ yes x no	

15	Does the emergency plan address the handling of ransomware, and is this plan also available in paper form?	□ yes x no	
16	Is the backup and recovery strategy reviewed to ensure that backups cannot be encrypted by ransomware?	□ yes x no	

16. Encryption

No.	Question	Answer	Explanation of Answer
1	Are clear rules defined for the effective use of cryptography, including key management?	x yes □ no	
2	Is the integrity of data, software, and IT systems ensured using current state-of-the-art hashing methods?	x yes □ no	
3	Is password storage using 'standard' hash functions (e.g. SHA class) only performed if the password is at least 12 characters long, and are salt values used to protect against rainbow table attacks?	□ yes x no	
4	Is password storage with salt performed in accordance with the current state of the art?	x yes □ no	PBKDF2
5	Is symmetric encryption performed in accordance with the current state of the art?	x yes □ no	
6	Is asymmetric encryption performed in accordance with the current state of the art?	x yes □ no	
7	Is effective key management (generation, issuance, revocation) in place when using cryptographic methods, and is it reviewed?	x yes □ no	
8	Are secret keys protected by strong passwords of at least 16 characters, and for high-risk situations, is the use of HSMs (Hardware Security Modules) considered?	□ yes x no	No HSM usage
9	Are SSL certificates obtained exclusively from trusted certification authorities?	x yes □ no	
10	Is HTTPS used in accordance with the current state of the art and is this verified?	x yes □ no	
11	Are cryptographic methods with known vulnerabilities or insufficient key lengths no longer used? If legacy systems still require these: Is this regularly reviewed and has an individual risk analysis been carried out?	□ yes x no	

17. Data Transfer

No.	Question	Answer	Explanation of Answer
1	Are clear rules in place for all types of internal data transfers as well as external data transfers outwards?	x yes □ no	Processing preferably within the EU; otherwise effective transfer mechanisms
2	Are procedures for the use of cloud services, including a possible exit strategy, established?	x yes □ no	
3	Are mobile data carriers such as DVDs, USB sticks, and hard drives encrypted in accordance with the current state of the art?	□ yes x no	Not used
4	For emails and cloud platforms: Is transport encryption of personal data ensured in accordance with the current state of the art for normal risk?	x yes □ no	
5	For emails and cloud platforms: Is transport and content encryption of personal data ensured in accordance with the current state of the art for high risk?	x yes □ no	

6	For messenger services: Are transport and content encryption of messages and files ensured?	x yes □ no	
7	Is the integrity of personal data ensured through digital signatures, at least for high-risk situations?	□ yes x no	
8	For HTTPS: Is the use of client certificates to verify authenticity within a closed user group taken into consideration?	x yes □ no	
9	Is encrypted use of DNS services (DNSSec, DNS-over-TLS) considered?	□ yes x no	

18. Software

No.	Question	Answer	Explanation of Answer
1	Are relevant employees trained that Security-by-Design (ensuring confidentiality, availability, and integrity) as a subset of Data-Protection-by-Design is a statutory data protection requirement that influences core design decisions?	x yes □ no	Privacy by Design & Default Guideline
2	Is there a separation between the production system and development/test systems?	x yes □ no	
3	Is access to the source code restricted during software development?	x yes □ no	
4	Is personal data or access credentials avoided in source code management?	x yes □ no	
5	Are system and security tests conducted?	x yes □ no	
6	Are sufficient test cycles taken into account?	x yes □ no	
7	Is continuous inventorying of the versions of software or components (e.g. frameworks, libraries) and their dependencies carried out?	x yes □ no	
8	Are standard software and corresponding updates only obtained from trusted sources?	x yes □ no	
9	Is it ensured that a continuous plan exists for monitoring, evaluating, and applying updates or configuration changes for the entire lifetime of a software application?	x yes □ no	

19. Data Processors (Processors pursuant to Art. 28 GDPR)

No.	Question	Answer	Explanation of Answer
1	Are only service providers used who can provide guarantees in the form of documents?	x yes □ no	In accordance with respective DPA
2	Are security measures pursuant to Art. 32 GDPR incorporated as part of a Data Processing Agreement (DPA) and adapted to the service?	x yes □ no	In accordance with respective DPA
3	Can the effectiveness of the guarantees be demonstrated (at least in part) by appropriate certifications?	x yes □ no	In accordance with respective DPA
4	Are on-site inspections by the controller not excluded?	x yes □ no	In accordance with respective DPA
5	Are processors prohibited from engaging further sub-processors without informing the controller, who then has at least a right to object?	x yes □ no	In accordance with respective DPA
6	Do processors have processes for detecting data protection breaches and do they report these to the controller without delay?	x yes □ no	In accordance with respective DPA

7	Are transfers to unsafe third countries only carried out with additional technical safeguards where applicable?	x yes □ no	In accordance with respective DPA
8	Is data effectively deleted during processing at the latest upon expiry of the contract?	x yes □ no	In accordance with respective DPA
9	Can information on the deletion methodology be provided upon request?	x yes □ no	In accordance with respective DPA
10	Is a regular review of processors regarding security practices and service delivery carried out?	x yes □ no	In accordance with respective DPA