Informationssicherheits- und Datenschutzkonzept

der WebAPP Anwendung TaskCards®

Information security and data protection concept of the WebAPP application TaskCards®

Stand/ Status 05.11.2022

Ersteller	Ersterstellung am:	Erstmalig Geprüft (Datum/Unterschrift)	Letztes Revisionsdatum	Klassifikation
K. Greibel	31.01.2022 DE_ENG_Vers	03.02.2022	04.11.2022	extern

Inhalt:

1. **Testat zur Sicherheit der Verarbeitung gemäß Art. 32 Datenschutz-Grundverordnung (DSGVO)**
2. **Spezifizierte technische und organisatorische Sicherheitsmaßnahmen der WebAPP TaskCards® gemäß Art 32 Datenschutzgrundverordnung (DSGVO)**

Content:

1. attestation / Assessment on the security of processing pursuant to Art. 32 of the General Data Protection Regulation (GDPR).

2. specified technical and organisational security measures of the WebAPP TaskCards® in accordance with Art. 32 of the General Data Protection Regulation (GDPR)

Einleitung / Introduction

Das Versprechen 100% datenschutzkonform eine Plattform in Deutschland zu betreiben, ist ein öffentliches Versprechen der Firma dSign Systems GmbH.

Die Konformität beginnt bereits bei Art. 12 DSGVO (EW 58). Dieses Transparenzgebot wollen wir nicht nur gegenüber Betroffenen, sondern auch gegenüber unseren Kunden, Interessenten und Lizenznehmern leben.

Die vorliegende Dokumentation Teil 1 *Testat zur Sicherheit der Verarbeitung gemäß Art. 32 Datenschutz-Grundverordnung (DSGVO)"* und Teil 2 *Spezifizierte technische und organisatorische Sicherheitsmaßnahmen der WebAPP TaskCards® gemäß Art. 32 Datenschutzgrundverordnung (DSGVO)* soll unser Versprechen unterstreichen.

The promise to operate a platform in Germany that is 100% compliant with data protection is a public promise by the company dSign Systems GmbH.

Conformity already starts with Art. 12 DSGVO (EW 58). We want to live this transparency requirement not only towards those affected, but also towards our customers, interested parties and licensees.

This documentation, Part 1 "Testate on the security of processing in accordance with Art. 32 of the General Data Protection Regulation (GDPR)" and Part 2 "Specified technical and organisational security measures of the WebAPP TaskCards® in accordance with Art. 32 of the General Data Protection Regulation (GDPR)", is intended to underline our promise.

Erläuterung / Explanation

Teil 1 Testat zur Sicherheit der Verarbeitung gemäß Art. 32 Datenschutz-Grundverordnung (DSGVO)

Das Testat beinhaltet die allgemeinen, grundsätzlichen, verfahrensübergreifende Technischen und organisatorischen Sicherungsmaßnahmen (TOM). Es wird hierbei unterschieden, ob dSign (UN) selbst oder ein von dSign beauftragter Dienstleister (DL) diese Maßnahmen sicherstellt.

Part 1 Attestation on the security of processing in accordance with Art. 32 of the General Data Protection Regulation (GDPR).

The attestation contains the general, fundamental, cross-procedural technical and organisational security measures (TOM). A distinction is made here as to whether dSign (UN) itself or a service provider commissioned by dSign (DL) ensures these measures.

Teil 2 Spezifizierte technische und organisatorische Sicherheitsmaßnahmen der WebAPP TaskCards® gemäß Art 32 Datenschutzgrundverordnung (DSGVO)

Die in Teil 2 aufgeführten Maßnahmen werden zusätzlich zu den allgemeinen, grundsätzlichen, technischen und organisatorischen Maßnahmen der Firma DSign Systems GmbH unter Zuhilfenahme ausgewählter Dienstleister umgesetzt.

Part 2 Specified technical and organisational security measures of the WebAPP TaskCards® in accordance with Art 32 of the General Data Protection Regulation (DSGVO).

The measures listed in Part 2 are implemented in addition to the general, fundamental, technical and organisational measures of DSign Systems GmbH with the assistance of selected service providers.

Beide Teile Zusammen bilden das Gesamtkonzept für Informationssicherheit und Datenschutz für die WebApp TAskCards®.

Both parts together form the overall concept for information security and data protection for the TAskCards® WebApp.

Für Fragen steht Ihnen unter datenschutz@dsign-systems.net einer unserer Experten gerne zur Verfügung.

If you have any questions, please do not hesitate to contact one of our experts at datenschutz@dsign-systems.net.

Testat zur Sicherheit der Verarbeitung

gemäß Art. 32 Datenschutz-Grundverordnung (DSGVO)

Certificate on the security of processing

in accordance with Art. 32 of the General Data Protection Regulation (DSGVO)

Stand / Status 04.11.2022

Einleitung / Introduction

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft dSign Systems GmbH folgende geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die beschriebenen, getroffenen und attestierten Maßnahmen sind an den Normenkatalog der CISIS12, weiterführend an die EN / ISO 27001 angelehnt und sollen ein angemessenes Schutzniveau erfüllen, um den durch die Prozesse ermittelten Schutzbedarf zu gewährleisten.

Das Testat beinhaltet die **allgemeinen, grundsätzlichen, verfahrensübergreifende Technischen und organisatorischen Sicherungsmaßnahmen (TOM)**. Es wird hierbei unterschieden, ob das u.g. Unternehmen (UN) oder ein Dienstleister für das Unternehmen (DL) diese Maßnahmen sicherstellt.

Der kontinuierlichen Verbesserungsprozess wird durch jährliche oder unterjährig bei Änderungen oder Incidents sichergestellt.

Taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, dSign Systems GmbH shall implement the following appropriate technical and organisational measures to ensure a level of protection appropriate to the risk.

The measures described, taken and certified are based on the CISIS12 catalogue of standards, and further on EN / ISO 27001, and are intended to provide an appropriate level of protection in order to ensure the need for protection determined by the processes.

The certificate contains the general, fundamental, cross-procedural technical and organisational security measures (TOM). A distinction is made here as to whether the company mentioned below (UN) or a service provider for the company (DL) ensures these measures.

The continuous improvement process is ensured by annual or intra-year audits in the event of changes or incidents.

Das Testat wird ausgestellt für das Unternehmen

The certificate is issued for the company

dSign Systems GmbH

Waldhausstraße 14

98574 Schmalkalden

Das Testat berücksichtigt die am Unternehmensstandort umgesetzten Sicherheitsmaßnahmen.	The attestation takes into account the security measures implemented at the company site.
Die Sicherheit der ortsfernen Server / Rechenzentren wird im Rahmen der Dienstleisterauswahl eingehend geprüft und im speziellen den jeweiligen Prozess / die jeweilige Anwendung betreffend in einem weiteren Dokument transparent dargestellt.	The security of the remote servers / data centres is checked in detail as part of the selection of the service provider and is presented transparently in a further document in relation to the respective process / application.
Das Unternehmen gewährleistet gemäß Art. 32 DSGVO folgende allgemeine, technischen und organisatorischen Sicherungsmaßnahmen:	The company ensures the following general, technical and organisational security measures in accordance with Art. 32 of the GDPR:

1. Management und Organisation / management and organisation

Mangelhafte Sicherheitsstrukturen in einer Organisation können den Betriebsablauf erheblich gefährden. Bestehende Fachkompetenzen sind daher zu nutzen. Dabei ist nicht nur der IT-Verantwortliche, sondern auch der Datenschutzbeauftragte (DSB) und Informationssicherheitsbeauftragte (ISB) im Prozess der Umsetzung von Sicherheitsanforderungen eingebunden.	Deficient security structures in an organisation can significantly jeopardise operations. Existing professional competences must therefore be utilised. Not only the IT officer, but also the data protection officer (DPO) and information security officer (IO) are involved in the process of implementing security requirements.

Management und Organisation / management and organisation

		durch	
		UN	DL
♦ Eine geeignete Organisationstruktur für Informationssicherheit ist vorhanden und die Informationssicherheit ist in die organisationsweiten Prozesse und Abläufe integriert Sicherheitsricht- und -leitlinien sind definiert, von der Geschäftsleitung genehmigt und dem Personal kommuniziert	♦ An appropriate organisational structure for information security is in place and information security is integrated into organisation-wide processes and procedures Security policies and guidelines are defined, approved by management and communicated to staff	☒	
♦ Die Rollen der einzelnen Mitarbeiter im Sicherheitsprozess sind eindeutig festgelegt	♦ The roles of the individual employees in the security process are clearly defined	☒	
♦ Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach dem PDCA-Zyklus	♦ Regular review of the effectiveness of the technical and organisational measures according to the PDCA cycle	☒	
♦ Konzepte und Dokumentationen im Sicherheitsumfeld werden regelmäßig überprüft und aktuell gehalten	♦ Concepts and documentation in the security environment are regularly reviewed and kept up to date.	☒	
♦ Je nach Unternehmensgröße: Einsatz eines geeigneten Informationssicherheitsmanagementsystem (ISMS), z. B. nach ISO/IEC 27001, BSI-Standards oder CISIS12	♦ Depending on the size of the company: use of a suitable information security management system (ISMS), e.g. according to ISO/IEC 27001, BSI standards or CISIS12	☒	
♦ Die Rollen und Verantwortlichkeiten im Bereich der Sicherheit sind im eigenen Betrieb bekannt und besetzt (u. a. Informationssicherheitsbeauftragter (ISB), IT-Leiter, Datenschutzbeauftragter (DSB))	♦ The roles and responsibilities in the area of security are known and filled within the company (e.g. information security officer (ISO), IT manager, data protection officer (DPO)).	☒	
♦ Konsequente Einbindung des DSB bei Sicherheitsfragen	♦ Consistent involvement of the DPO in security issues	☒	
♦ Ausreichende fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema	♦ Adequate professional qualification of the DPO for security-relevant issues and opportunities for further training on this topic	☒	
♦ Ausreichende fachliche Qualifikation des ISB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema	♦ Adequate professional qualification of the DPO for security-related issues and opportunities for further training on this topic	☒	
♦ Durchführung von regelmäßigen Audits des DSB nach Art. 32 DS-GVO zur Sicherheit der Verarbeitung	♦ Carrying out regular audits of the DPO in accordance with Art. 32 of		

	the GDPR on the security of processing		
♦ Durchführung von regelmäßigen internen Audits des ISB zur Sicherheit der Verarbeitung	♦ Implementation of regular internal audits of the ISB on the security of processing.	☒	
♦ Kenntnis der zuständigen Datenschutzaufsichtsbehörde sowie Wissen über die Meldeverpflichtungen nach Art. 33 und 34 DS-GVO (Verletzung der Sicherheit)	♦ Knowledge of the competent data protection supervisory authority as well as knowledge of the notification obligations pursuant to Art. 33 and 34 of the GDPR (breach of security)	☒	
♦ Vorhandensein von Eskalationsprozessen bei Sicherheitsverletzungen (Wer ist wann wie zu informieren?), u. a. im Notfallmanagement	♦ Existence of escalation processes in the event of security breaches (who is to be informed when and how?), among other things in emergency management	☒	
♦ Konsequente Dokumentation bei Sicherheitsvorkommnissen (Security Reporting)	♦ Consistent documentation of security incidents (security reporting)		☒
♦ Aktive Unterstützung der Zusammenarbeit des DSB mit dem ISB durch die Unternehmensleitung	♦ Active support of the DPO's cooperation with the IPM by the company management.	☒	
♦ Erkenntnisse über (neue) digitale Bedrohungen sind zu sammeln und potenzielle Auswirkungen auf den eigenen Betrieb abzuleiten	♦ Insights into (new) digital threats are to be gathered and potential effects on the company's own operations are to be deduced	☒	

2. Physikalische Sicherheit der Infrastruktur / physical protection of the infrastructure

Der persönliche Zugang zu IT-Systemen und personenbezogenen Daten muss Unbefugten erschwert werden. Ebenso sind gravierende Schäden durch (Natur-)Ereignisse wie Feuer oder Wasser bestmöglich zu verhindern.	Personal access to IT systems and personal data must be made difficult for unauthorised persons. Likewise, serious damage caused by (natural) events such as fire or water must be prevented as best as possible.

Physikalische Sicherheit der Infrastruktur / physical protection of the infrastructure		durch	
		UN	DL
♦ Es besteht ein Konzept zu Zutrittsregelungen und zur physischen Zugangskontrolle (Perimeterschutz)	♦ A concept for access regulations and physical access control (perimeter protection) is in place.	☒	
♦ Klare Regelungen zum Umgang mit Besuchern (z. B. Begleitung,	♦ Clear regulations on dealing with visitors (e.g. escorts, safety zones,	☒	

Sicherheitszonen, Besucherausweise, Protokollierung, Zuständiger Mitarbeiter für Besucher) als Bestandteil des Konzeptes	visitor passes, logging, responsible staff member for visitors) as a component of the concept.		
♦ Gelebte Regelungen zum Umgang auch mit externen Dienstleistern (z. B. bei Werkverträgen, Handwerker, Wartung von Systemen) – wie Verschwiegenheitserklärung, persönliche Begleitung in Sicherheitszonen oder Protokollierung	♦ Practical rules for dealing with external service providers (e.g. contracts for work, craftsmen, maintenance of systems) - such as confidentiality agreement, personal escort in security zones or logging.	☒	
♦ Schaffung von verschiedenen Sicherheitszonen (z. B. Besucherbesprechungen, Serverräume, Arbeitsplätze, Forschungsbereich)	♦ Creation of different security zones (e.g. visitors' meetings, server rooms, workplaces, research area).	☒	
♦ Sichere Schließsysteme samt dokumentierter Schlüsselverwaltung	♦ Secure locking systems including documented key management	☒	
♦ Das Gebäude (z. B. Wände, Fenster) und die Infrastruktur (z. B. Leitungen, Gefahrenmeldeanlagen) werden regelmäßig geprüft und gewartet	♦ The building (e.g. walls, windows) and the infrastructure (e.g. pipes, hazard detection systems) are regularly inspected and maintained.	☒	
♦ Umzäunung des Betriebsgeländes	♦ Fencing of the premises	☒	
♦ Ausreichende Klimatisierung von Serverräumen	♦ Sufficient air conditioning of server rooms	☒	
♦ Einsatz von Anlagen zur Sicherstellung der Stromversorgung von Serversystemen (unterbrechungsfreie Stromversorgung (USV)), insbesondere bei kurzfristigen Stromausfällen oder Schwankungen	♦ Use of systems to ensure the power supply of server systems (uninterruptible power supply (UPS)), especially in the event of short-term power failures or fluctuations	☒	
♦ Absicherung der Gebäudeschächte (z.B. Lichtschächte vor Kellerfenstern)	♦ Securing building shafts (e.g. light shafts in front of basement windows)	☒	
♦ Türen in sensiblen Bereichen mit Knauf an der Außenseite	♦ Doors in sensitive areas with thumb turn on the outside	☒	
♦ Risiken durch Überflutung/Starkregen geprüft, insbesondere bei Serverräumen im	♦ Checked risks due to flooding/ heavy rain, especially for server	☒	

Keller oder anderen gefährdeten Bereichen	rooms in the basement or other vulnerable areas		
♦ Sorgfalt bei Auswahl der Reinigungsdienste	♦ Due diligence in the selection of cleaning services	☒	

3. Awareness der Mitarbeiter / awareness of the employees

Beschäftige stehen mittlerweile verstärkt im Fokus von Cyberattacken. Mittels raffinierten Social Engineering Techniken sollen sie dazu verleitet werden, sicherheitskritische Aktionen auszuführen. Mitarbeiterawareness ist gerade in Sicherheitsfragen wichtig, um solche Angriffe zu vereiteln.

Employees are now increasingly the focus of cyberattacks. Sophisticated social engineering techniques are used to trick them into performing security-critical actions. Employee awareness is particularly important in security matters in order to thwart such attacks.

Awareness der Mitarbeiter / awareness of the employees		durch	
		UN	DL
♦ Das gesamte Personal der Organisation hat eine angemessene Schulung für Informationssicherheit und Datenschutz erhalten, soweit dies für die jeweilige Funktion relevant ist	♦ All employees of the organisation have received appropriate training in information security and data protection, as relevant to their function	☒	
♦ Anleitung „Manuelle Desktopsperre" ist den Mitarbeitern bekannt und wird angewendet	♦ Manual desktop lock" instructions are known to employoyees and applied	☒	
♦ Datenschutz- und Informatiossicherheitsschulungen für neue Beschäftigte zeitnah nach Aufnahme des Beschäftigungsverhältnisses	♦ Data protection and information security training for new employees promptly after the start of employment	☒	
♦ Regelmäßige Auffrischungsschulungen für bestehendes Personal (z. B. einmal pro Jahr)	♦ Regular refresher training for existing employoyees (e.g. once a year)	☒	
♦ Regelmäßige Informationen im Betrieb an alle über Neuigkeiten zum Datenschutz und der IT-Sicherheit (z. B. per Mail, Intranet, Kollaborationsplattform, Aushang)	♦ Regularly inform everyone in the company about news on data protection and IT security (e.g. by email, intranet, collaboration platform, notice board).	☒	
♦ Schulungsinhalte: Beschäftigten lernen kennen, wie Cyberangriffe mittels Social-Engineerings	♦ Training content: Employees learn how cyber attacks are initiated by	☒	

eingeleitet werden (Hilfe zur Selbsthilfe)	means of social engineering (help for self-help)		
♦ Schulungsinhalte: Beschäftigten erfahren von den Gefahren der E-Mail-Kommunikation, insbesondere bei verschlüsselten E-Mail-Anhängen (z. B. Zip-Datei mit Passwort)	♦ Training content: Employees learn about the dangers of email communication, especially with encrypted email attachments (e.g. zip file with password).	☒	
♦ Schulungsinhalte: Beschäftigten erkennen gefälschte E-Mails (z. B. Absenderadressen, Auffälligkeiten, eingebettete Links)	♦ Training content: Employees recognise fake emails (e.g. sender addresses, conspicuousness, embedded links).	☒	
♦ Sensibilisierung des Personals, das mit Externen wie z. B. Lieferanten interagiert, in Bezug auf angemessene Einsatzregeln, Richtlinien, Prozesse und Verhalten (u. a. welche Daten dürfen in welcher Form weitergegeben werden, was kann sicherheitskritisch sein)	♦ Raise awareness of employeyees interacting with external parties, such as suppliers, on appropriate rules of engagement, policies, processes and behaviour (including what data may be shared and in what form, what may be security sensitive).	☒	
♦ Von Homeoffice betroffenen Mitarbeiter werden die sichere Nutzung von „Homeoffice" (Mobiles Arbeiten) Lösungen erläutert und spezifische Gefahren aufgezeigt	♦ Employees affected by working from home will have the safe use of "home office" (mobile working) solutions explained and specific hazards highlighted.	☒	

4. Authentifizierung / authentication

Digitale Zugangsbeschränkungen helfen im Alltag. Nutzer von IT-Systemen und Diensten müssen daher Ihre Zugangsberechtigung mit geeigneten Mitteln nachweisen.	Digital access restrictions help in everyday life. Users of IT systems and services must therefore prove their access authorisation by suitable means.

Authentifizierung / authentication		durch	
		UN	DL
♦ Einweisung aller Mitarbeiter in den Umgang mit Authentifizierungsverfahren und -mechanismen	♦ Instructing all employees in the use of authentication procedures and mechanisms	☒	

♦ Vergabe von eindeutigen Kennungen für jeden Nutzer Vermeidung von Gruppenkennungen	♦ Assignment of unique identifiers for each user Avoidance of group identifiers	☒
♦ Bei zwingender Nutzung von Gruppenkennungen: Einsatz von datenschutzkonformer Protokollierung der dazugehörigen Nutzeraktivitäten	♦ Bei zwingender Nutzung von Gruppenkennungen: Einsatz von datenschutzkonformer Protokollierung der dazugehörigen Nutzeraktivitäten	☒
♦ Verwendung von starken Passwörtern und Veröffentlichung einer Richtlinie dafür – z. B. mind. 10-tellig bei zufälligen komplexen Zeichen oder mind. 16-stellig bei einfacheren Zeichenfolgen ohne direkte Verwendung von üblichen Wörtern	♦ Use strong passwords and publish a guideline for them - e.g. at least 10 digits for random complex characters or at least 16 digits for simpler strings without direct use of common words.	☒
♦ Möglichst automatische Umsetzung der Passwortrichtlinie für starke Passwörter in den Systemen mit Nutzerkennungen	♦ Implement the password policy for strong passwords in the systems with user IDs as automatically as possible.	☒
♦ Verhinderung der Auswahl schwacher Passwörter bei Anwendungen (z. B. über Richtlinien oder technisch erzwungen über das Identity Management System)	♦ Preventing the selection of weak passwords in applications (e.g. via policies or technically enforced via the identity management system).	☒
♦ Ggf. Überprüfung der Regel, dass Passwörter nach festgelegten Zeiträumen (z. B. 60 Tage) geändert werden müssen – falls diese Passwörter „stark" sind, kann ein anlassloses Passwortwechselintervall deutlich länger ausfallen (z. B. einmal pro Jahr)	♦ If necessary, review the rule that passwords have to be changed after fixed periods (e.g. 60 days) - if these passwords are "strong", a no-cause password change interval can be significantly longer (e.g. once a year).	☒
♦ Passwörter werden nach einem Sicherheitsvorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden	♦ Passwords are blocked after a security incident, even if suspected, and must be reassigned by the user	☒
♦ Bei erstmaligem Login eines neuen Nutzers oder Zurücksetzung des Passworts durch IT (z. B. bei Vergessen des Passworts) muss eine Passwortänderung durch den Nutzer erfolgen	♦ When a new user logs in for the first time or the password is reset by IT (e.g. if the password is forgotten), the user must change the password.	☒

♦ Passwörter dürfen nicht weitergegeben werden (auch nicht an Kollegen, Vorgesetze oder die IT-Abteilung) – im Ausnahmefall (z. B. längere Erkrankung) wird das Passwort durch die IT zurückgesetzt und dieser Vorgang dokumentiert	♦ Passwords must not be passed on (not even to colleagues, superiors or the IT department) - in exceptional cases (e.g. longer illness) the password is reset by IT and this process is documented	☒	
♦ Unterrichtung der Beschäftigten, dass Passwörter nicht auf Zettel oder Pinnwänden aufgezeichnet werden dürfen	♦ Teaching employees that passwords must not be recorded on slips of paper or noticeboards	☒	
♦ Keine Speicherung von Passwörtern im Browser ohne Sicherung durch ein Masterpasswort	♦ No saving of passwords in the browser without securing them with a master password	☒	
♦ Keine Mehrfachverwendung eines Passworts für verschiedene Dienste, sofern kein zentrales Identitätsmanagement (z. B. Active Directory) verwendet wird	♦ No multiple use of a password for different services unless central identity management (e.g. Active Directory) is used.	☒	
♦ Für lokale Admin-Konten besonders starke Passwörter (z. B. mind. 16-stellig, komplex und ohne übliche Wortbestandteile sowie unterschiedlich für jeden PC)	♦ For local admin accounts, particularly strong passwords (e.g. at least 16 digits, complex and without common word components, and different for each PC).	☒	
♦ Automatische Sperrung von Zugängen bei zu vielen Fehlversuchen durch falsches Passwort: Entweder zeitbasiert (eine Stunde, sechs Stunden, 24 Stunden) oder komplett (Kontaktaufnahme mit IT notwendig)	♦ Automatic blocking of accesses in case of too many failed attempts due to wrong password: Either time-based (one hour, six hours, 24 hours) or complete (contacting IT necessary)	☒	
♦ Zeitverzögerung zwischen einzelnen Login-Versuchen (insbesondere bei über das Internet erreichbaren Anwendungen) zur Erschwerung von automatischen Online-Angriffen	♦ Time delay between individual login attempts (especially for applications accessible via the Internet) to make automatic online attacks more difficult	☒	
♦ Darstellung der Anzahl der fehlgeschlagenen Logins für einen Nutzer, der sich erfolgreich anmeldet. Ziel: Transparenz für stattgefundene Angriffe bzw. Angriffsversuche schaffen.	♦ Display of the number of failed logins for a user who successfully logs in. Objective: To create transparency for attacks or attempted attacks that have taken place.	☒	

♦ Passwörter nicht im Klartext speichern, sondern geeignete kryptographische Verfahren einsetzen (z. B. bcrypt mit Salt)	♦ Do not store passwords in plain text, but use suitable cryptographic procedures (e.g. bcrypt with Salt).	☒	
♦ Regelungen zum automatischen Sperren von Passwörtern nach einem Sicherheitsvorfall treffen (z. B. Passwort-Hash so abändern, dass kein Klartextpasswort dazu besteht)	♦ - Established rules for automatically locking passwords after a security incident (e.g. change password hash so that no clear text password exists for it).	☒	
♦ Standard-Authentifizierungsinformationen durch Hersteller bei Software werden nach der Installation geändert	♦ Default authentication information by manufacturer for software is changed after installation	☒	

5. Rollen-/Rechtekonzept - roles/rights concept

Nutzer sollen nur auf die personenbezogenen Daten zugreifen können, die für ihre Tätigkeit erforderlich sind. Durch Einführung von Benutzerrechten zu bestimmten Rollen (z. B. Buchhaltung, IT-Administration) werden unterschiedliche Rechte an konkrete Personen zugewiesen.	Users should only be able to access personal data that is necessary for their activities. By introducing user rights to specific roles (e.g. accounting, IT administration), different rights are assigned to specific persons.

Rollen-/Rechtekonzept - roles/rights concept		durch	
		UN	DL
♦ Erstellen von Rollenprofilen für die Beschäftigten unter Einbeziehung der Einträge des Verzeichnisses der Verarbeitungstätigkeiten	♦ Create role profiles for the employees including the entries of the register of processing activities	☒	
♦ Regelungen zur Verwaltung der Rollen (Zuweisung, Entzug) an die Mitarbeiter etabliert	♦ Regulations established for the administration of roles (assignment, withdrawal) to employees	☒	
♦ Regelmäßige Überprüfung (z. B. einmal pro Jahr), ob die Zuweisung der Rollen den Vorgaben entspricht sowie, ob die Rollen noch den Anforderungen der Geschäftstätigkeit entspricht	♦ Regularly review (e.g. once a year) whether the assignment of roles is in accordance with the specifications as well as whether the roles still meet the requirements of the business activity	☒	
♦ Verwaltung Benutzerrechte ausschließlich durch Administratoren	♦ Management of user rights exclusively by administrators	☒	

♦ Keine Administratorkennungen für Nutzer, die keine administrativen Tätigkeiten ausführen	♦ No administrator IDs for users who do not perform administrative tasks	☒	
♦ Verschiedene administrative Rollen (z. B. Anlage neuer Benutzer, Durchführung von Backups, Konfiguration der Firewall) für die IT-Administration erstellt	♦ Created various administrative roles (e.g. creating new users, performing backups, configuring the firewall) for IT administration.	☒	
♦ Für Beschäftigte mit IT-Administrationsaufgaben zwei Benutzerkennungen eingerichtet: eine Administrationskennung und eine normale Nutzerkennung (für nicht-administrative Zwecke wie z. B. das Surfen im Internet)	♦ Two user IDs set up for employees with IT administration tasks: an administration ID and a normal user ID (for non-administrative purposes such as surfing the Internet)	☒	

6. Endgeräte / Clients

Die für die tägliche Arbeit genutzten Endgeräte der Nutzer müssen dauerhaft abgesichert werden. Keine oder nur unzureichende Regelungen führen meist zu offenen Schwachstellen auf Clientsystemen, von denen dann eine erhebliche Gefährdung für die gesamte Organisation ausgehen kann.	The end devices of the users used for daily work must be permanently secured. No or only insufficient regulations usually lead to open vulnerabilities on client systems, which can then pose a considerable threat to the entire organisation.

Endgeräte / Clients		durch	
		UN	DL
♦ Eine Geräteverwaltung (Wer setzt welche Geräte in welchem Bereich ein?) ist vorhanden	♦ A device management (who uses which devices in which area?) is available	☒	
♦ Automatisches Sperren nach einer gewissen Zeitspanne der Inaktivität, falls manuelles Sperren bei Verlassen des Einflussbereichs nicht gewährleistet werden kann	♦ Automatically locks after a certain period of inactivity if manual locking cannot be guaranteed when leaving the sphere of influence	☒	
♦ Aktivierung einer Firewall, die unerwünschte Servicedienste auf dem Endgerät blockiert (z. B. versehentlich installierter Webserver)	♦ Activation of a firewall that blocks unwanted services on the end device (e.g. inadvertently installed web server).	☒	

♦ Verwendung einer Anti-Viren-Lösung bzw. eines Endpoint-Protection-Systems mit regelmäßigen, mindestens tagesaktuellen Signatur-Updates und Regelungen, wie im Falle einer Warnmeldung zu verfahren ist	♦ Application of an anti-virus solution or an endpoint protection system with regular signature updates that are updated at least daily and regulations on how to proceed in the event of a warning message.	☒	
♦ Zentrale Erfassung von Schadcode-Alarmmeldungen durch die IT-Administration	♦ Central registration of malware alerts by the IT administration	☒	
♦ Konzept zum Patch Management vorhanden (u. a. UpdatePlan mit Übersicht der eingesetzten Software)	♦ Patch management concept in place (including an update plan with an overview of the software in use).	☒	
♦ Regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software und Fachanwendungen (z. B. durch E-Mail-Newsletter, Herstellerveröffentlichungen, Fachmedien, Sicherheitswarnungen)	♦ Periodic evaluation of information on security vulnerabilities in the software used, such as operating systems, office software and specialist applications (e.g. through e-mail newsletters, manufacturer publications, specialist media, security warnings).	☒	
♦ Automatisches Einspielen von Sicherheitsupdates des Betriebssystems, der installierten Software (z. B. PDF-Reader) oder von Softwarebibliotheken (z. B. Java), sofern möglich	♦ Automatic installation of security updates of the operating system, the installed software (e.g. PDF reader) or software libraries (e.g. Java), if possible.	☒	
♦ Personenbezogene Daten werden auf einem Speichermedium gespeichert werden, das von dem Backup erfasst wird (z. B. Netzlaufwerk)	♦ Personal data will be stored on a storage medium that is covered by the backup (e.g. network drive).	☒	
♦ Einbindung von externen Geräten durch technische Maßnahmen auf das erforderliche Mindestmaß begrenzen (z. B. bei USB-Sticks, Smartphones, externe Festplatten)	♦ Limit the integration of external devices to the minimum necessary through technical measures (e.g. USB sticks, smartphones, external hard drives).	☒	
♦ Fernwartung für Clients zu IT-Administrationszwecken ausschließlich über verschlüsselte Verbindungen nach Authentifizierung durch den	♦ Remote maintenance for clients for IT administration purposes exclusively via encrypted connections after authentication by	☒	

Administrator und Freigabe durch den Nutzer	the administrator and release by the user		
♦ Nur Betriebssysteme und Software eingesetzt, für die noch Sicherheitsupdates zeitnah zur Verfügung gestellt werden	♦ Only operating systems and software used for which security updates are still made available in a timely manner	☒	
♦ Gehäuseverriegelung an Serverschränken, um unbefugten Zugriff auf Speichermedien zu verhindern	♦ Enclosure locking on server cabinets to prevent unauthorised access to storage media	☒	
♦ Der Zugang zu Websites sollte restriktiv verwaltet werden, sodass das Risiko einer Kompromittierung z. B. durch Malware verringert und der Zugriff auf nicht autorisierte Websites verhindert wird (z. B. über Web-Proxy mit aktuellen Sperrlisten)	♦ Access to websites should be managed restrictively so that the risk of compromise, e.g. by malware, is reduced and access to unauthorised websites is prevented (e.g. via web proxy with up-to-date blacklists)	☒	
♦ Anwendungen werden an den Endgeräten möglichst ohne Administratorrechte ausgeführt	♦ Applications are run on the end devices without administrator rights if possible	☒	
♦ Prozess zur wirksamen Datenlöschung vor Vergabe eines Endgeräts an einen anderen Mitarbeiter aufsetzen	♦ Establish a process for effective data deletion before handing over a terminal to another employee.	☒	
♦ Ein Sicherheitskonzept für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten ist vorhanden (z. B. keine unerlaubte Einsicht in ausgedruckte Dokumente, ausreichender Schutz gespeicherter Informationen, ordnungsgemäße Entsorgung)	♦ A security concept for the use of printers, copiers and multifunctional devices is in place (e.g. no unauthorised viewing of printed documents, adequate protection of stored information, proper disposal).	☒	

7. Mobile Datenspeicher / Mobile data storage

Der weit verbreitete Einsatz von USB-Datenträgern, Notebooks und Smartphones macht Regelungen zur Nutzung und auch für den Verlustfall erforderlich. Ungeschützte Speichermedien ermöglichen ansonsten Unbefugten ohne großen Aufwand Zugriff auf sensible Daten.	The widespread use of USB data carriers, notebooks and smartphones makes regulations necessary for their use and also in the event of loss. Unprotected storage media otherwise allow unauthorised persons to access sensitive data without much effort.

Mobile Datenspeicher / Mobile data storage		durch	
		UN	DL
♦ Einsatz starker Verschlüsselung der mobilen Endgeräte (z. B. Festplattenverschlüsselung, Container-Lösungen)	♦ Use strong encryption of mobile devices (e.g. hard disk encryption, container solutions).	☒	
♦ Einsatz von Backup- und Synchronisierungsmechanismen zur Verhinderung eines größeren Datenverlusts bei Verlust und Diebstahl	♦ Use of backup and synchronisation mechanisms to prevent major data loss in case of loss and theft	☒	
♦ Bei Smartphones: Zugang ausschließlich nach Authentifizierung (z. B. PIN, Passwort) – Länge der Kennung in Abhängigkeit von automatischen Sperr- und Löschfunktionen	♦ For smartphones: access only after authentication (e.g. PIN, password) - length of identifier depending on automatic locking and deletion functions	☒	
♦ Bei Smartphones: Einsatz von biometrischen Zugangsverfahren nur bei ausschließlich lokaler Speicherung der biometrischen Templates innerhalb eines Secure-Chips auf dem Smartphone und bei personenbezogenen Daten mit keinem hohen Risiko	♦ For smartphones: Use of biometric access methods only with exclusively local storage of the biometric templates within a secure chip on the smartphone and for personal data with no high risk	☒	
♦ Bei Smartphones: Cloud-Speicher für Datenbackup erst nach sorgfältiger Prüfung der datenschutzrechtlichen Anforderungen einsetzen (auch Beschäftigtendatenschutz bei „Find my Phone"-Funktionen)	♦ For smartphones: Use cloud storage for data backup only after careful examination of the data protection requirements (also employee data protection for "Find my Phone" functions).	☒	
♦ Bei Smartphones: Nur sichere Quellen werden für die Installation von Apps verwendet. Apps werden vorher getestet und freigegeben	♦ For smartphones: Only secure sources are used for installing apps. Apps are tested and approved beforehand	☒	
♦ Regelungen prüfen, ob es ausreichend ist, bei Nutzung mobiler Arbeitsplätze (z. B. Notebook auf Dienstreise) auf weniger Daten als innerhalb des internen Unternehmensnetzes zugreifen zu können Diebstahlsicherungen (z. B.	♦ Check whether it is sufficient to be able to access less data than within the internal company network when using mobile workstations (e.g. notebook on business trip) Provide anti-theft devices (e.g. installation of	☒	

Anbringung von verschließbaren Stahlkabeln) für Notebooks bei Bedarf zur Verfügung stellen	lockable steel cables) for notebooks if required.		
♦ Regelungen zur Privatnutzung bei Notebooks und Smartphones geschaffen - Keine Privatnutzung	♦ Regulations on private use created for notebooks and smartphones - No private use	☒	
♦ Die Mitarbeiter kennen die Regelungen bei Verlust eines mobilen Endgerätes, z. B. Verlustmeldung beim Unternehmen und/oder Polizei	♦ Employees know the regulations in case of loss of a mobile device, e.g. report the loss to the company and/or the police.	☒	

8. Serversysteme / Serversysteme

Serversysteme müssen mit besonderer Sorgfalt abgesichert werden, da Sicherheitsverletzungen dort i. d. R. aufgrund der großen Menge personenbezogener Daten enorme Auswirkungen haben können.	Server systems must be secured with special care, as security breaches there can usually have enormous consequences due to the large amount of personal data.

Serversysteme / Serversysteme		durch	
		UN	DL
♦ Nur kompetent geschulte Personen dürfen Administrationstätigkeiten auf den Servern durchführen	♦ Only competently trained persons may carry out administrative activities on the servers	☒	
♦ Verschiedene Administrationsrollen mit Rechten nach dem Least-Privileg-Prinzip für unterschiedliche Administrationsaufgaben (z. B. Softwareupdates, Konfiguration, Backup) einsetzen	♦ Use different administration roles with rights according to the least privilege principle for different administration tasks (e.g. software updates, configuration, backup).	☒	
♦ Geregelter Prozess zum zeitnahen Einspielen von Sicherheitsupdates der Server – kritische Updates müssen unverzüglich eingespielt werden	♦ Regulated process for the prompt installation of server security updates - critical updates must be installed immediately	☒	
♦ Deaktivierung/Deinstallation von Standard Server-Diensten, die nicht benötigt werden (z. B. Webserver, Printserver)	♦ Deactivation/uninstallation of standard server services that are not needed (e.g. web server, print server)	☒	

♦ Serverlokale Dienste über Firewall auf Servern vor Außenzugriff blockieren	♦ Block local server services from external access via firewall on servers	☒	
♦ Serverraumüberwachung mit Sensoren für Temperatur und Feuchtigkeit	♦ Server room monitoring with sensors for temperature and humidity	☒	
♦ Verwendung von Schutzsteckdosen im Serverraum mit Überspannungsschutz	♦ Use of protective sockets in the server room with overvoltage protection	☒	
♦ Installation RAID System / Festplattenspiegelung werden regelmäßig durchgeführt	♦ Installation RAID system / hard disk mirroring are carried out regularly	☒	
♦ Keine sanitären Anschlüsse im oder oberhalb des Archivs	♦ No sanitary connections in or above the archive	☒	
♦ Brandschutztüren insbesondere vor den sensiblen Bereichen	♦ Fire protection doors especially in front of the sensitive areas	☒	

9. Websites und Webanwendungen / Websites and Webapplication

Webseiten und Webanwendungen stellen meist leicht zugängliche Plattformen für Angriffe dar, die mit bekannten Best-Practice-Ansätzen meist gut abgesichert werden können.	Websites and web applications are usually easily accessible platforms for attacks, which can usually be well secured with known best practice approaches.

Websites und Webanwendungen / Websites and Webapplication		durch	
		UN	DL
♦ Verwendung des HTTPS-Protokolls nach Stand der Technik (TLS1.2 oder TLS1.3)	♦ Using the HTTPS protocol according to the state of the art (TLS1.2 or TLS1.3)	☒	
♦ Absicherung von Datenbanken auf dem Webserver mittels Firewalls	♦ Securing databases on the web server using firewalls	☒	☒
♦ Fernzugang zu Webservern nur mit verschlüsselter Verbindung und Zwei-Faktor-Authentifizierung (z. B. SSH mit Client-Zertifikaten)	♦ Remote access to web servers only with encrypted connection and two-factor authentication (e.g. SSH with client certificates)		☒
♦ Limitierung von Administrationsbereichen der Webanwendungen auf bestimmte IP-Adressen (z. B. Unternehmens-Gateway)	♦ Limitation of administration areas of the web applications to certain IP addresses (e.g. company gateway)	☒	

♦ Nur geschulte bzw. kompetente Personen dürfen Administrationstätigkeiten auf den Servern durchführen	♦ Only trained or competent persons may carry out administrative activities on the servers.	☒	
♦ Geregelter Prozess zur Information über Sicherheitsupdates und zeitnahes Einspielen derselben, insbesondere bei gängigen Content-Management-Systemen (CMS)	♦ Regulated process for informing about security updates and promptly installing them, especially for common content management systems (CMS)	☒	
♦ Keine Übertragung personenbezogener Daten (z. B. Mail Adresse) per HTTP-GET-Request, da diese in den Webserver-Log-Dateien gespeichert werden und durch eingesetzte Website-Tracker ausgeleitet werden können	♦ No transmission of personal data (e.g. mail address) via HTTP GET request, as this is stored in the web server log files and can be diverted by the website trackers used.		☒
♦ Trennung von Webserver, Anwendungslogik und Datenhaltung einer Webanwendung durch eigene Server, die in eine geeignete Firewall-Architektur (z. B. DMZ – Demilitarisierte Zone) eingebunden sind	♦ Separation of web server, application logic and data storage of a web application by own servers which are integrated into a suitable firewall architecture (e.g. DMZ - Demilitarised Zone).	☒	
♦ Sperrung der Auffindung von Inhalten durch Suchmaschinen (über robots.txt), sofern diese Inhalte nicht durch eine Suchmaschine gefunden werden sollen,	♦ Block search engines from finding content (via robots.txt) if this content is not to be found by a search engine	☒	

10. Netzwerk / network

Angriffe über das Internet auf das eigene Netzwerk sind in vielen Organisationen möglich. Damit sich dadurch z. B. kein Schadcode ausbreiten kann, ist die eigene Netzwerkstruktur vor solchen negativen Fremdeinflüssen aktiv zu schützen.	Attacks on one's own network via the internet are possible in many organisations. To prevent the spread of malicious code, for example, one's own network structure must be actively protected against such negative external influences.

Netzwerk / network		durch	
		UN	DL
♦ Geeignete Netzwerksegmentierung durchgeführt: Restriktive	♦ Implemented appropriate network segmentation: Restrictive (physical)	☒	

(physikalische) Trennung sensitiver Netze von Verwaltungsnetzen (mittels Firewall-Systemen)	separation of sensitive networks from administrative networks (using firewall systems).		
♦ Einsatz einer Firewall am zentralen Internetübergang	♦ Use a firewall at the central Internet gateway	☒	☒
♦ Blockierung aller nicht benötigten Dienste (z. B. VoIP, Peer-to-Peer, Telnet)	♦ Blocking of all unneeded services (e.g. VoIP, Peer-to-Peer, Telnet)	☒	
♦ Einsatz geeigneter Firewall-Architekturen zur Absicherung rein interner Systeme (z. B. Arbeitsplatz, Drucker) zu den über das Internet erreichbaren Servern (z. B. Mail-Server, Web-Server, VPN-Endpunkt)	♦ Use of suitable firewall architectures to secure purely internal systems (e.g. workstation, printer) to servers accessible via the Internet (e.g. mail server, web server, VPN endpoint)	☒	
♦ Einsatz von Funkzugängen per WLAN nur auf aktuellen WLAN-Routern mit wirksamen Zugangsmechanismen (z. B. WPA-2 mit mind. 24-stelligem Passwort, WP3-Enterprise oder Einsatz eines Radius-Servers)	♦ Use of wireless access via WLAN only on current WLAN routers with effective access mechanisms (e.g. WPA-2 with at least 24-digit password, WP3-Enterprise or use of a Radius server).	☒	
♦ Nutzung eines WLAN-Gastzugang ohne Zugangsmöglichkeit zum internen Netzwerk	♦ Use of a WLAN guest access without access to the internal network	☒	
♦ Protokollierungen auf Firewall-Ebene, um auch unbefugte Zugriffe zwischen den Netzen festzustellen und zu analysieren	♦ Logging at firewall level to also detect and analyse unauthorised access between networks	☒	
♦ Automatische Benachrichtigungen an die IT-Administration bei Verdacht auf unbefugte Verarbeitungen	♦ Automatic notifications to the IT administration if unauthorised processing is suspected	☒	
♦ Regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall (z. B. mittels Portscans)	♦ Regularly check the correct configuration of the firewall (e.g. by means of port scans)	☒	
♦ Einsatz von ausreichend qualifiziertem Personal/Dienstleister zur Konfiguration der Firewall	♦ Use of sufficiently qualified personnel/service provider to configure the firewall	☒	☒
♦ Prüfung eingehender E-Mails mittels Anti-Malwareschutz	♦ Checking incoming e-mails using anti-malware protection	☒	
♦ Blockieren von gefährlichen Email-Anhängen (z. B. .exe, .doc, .cmd)	♦ Blocking dangerous email attachments (e.g. .exe, .doc, .cmd)	☒	

♦ Anbindung von Niederlassungen oder Homeoffice über stark verschlüsselte VPN-Verbindungen	♦ Connection of branch offices or home offices via strongly encrypted VPN connections	☒	

11. Archivierung / archiving

Archivdaten werden zwar für die tägliche Arbeit nicht mehr benötigt, müssen aber mitunter aufgrund gesetzlicher Aufbewahrungsfristen eine bestimmte Zeit lang weiterhin aufbewahrt werden. Eine Absicherung der enthaltenen personenbezogenen Daten ist daher auch dann zu gewährleisten.	Although archive data is no longer needed for daily work, it must sometimes continue to be stored for a certain period of time due to legal retention periods. Safeguarding the personal data it contains must therefore also be ensured then.

Archivierung / archiving		durch	
		UN	DL
♦ Regelungen etabliert, welche Daten auf welcher Rechtsgrundlage aufbewahrt werden müssen und wie lange die Aufbewahrungsfrist ist	♦ Regulations established as to which data must be retained on which legal basis and how long the retention period is	☒	
♦ Zugänge zu den Archivdateien festlegen: Dokumentieren, Umsetzen und Prüfen	♦ Determine access to the archive files: Document, convert and check	☒	
♦ Archivdaten müssen nach Ablauf der Aufbewahrungsfrist wirksam gelöscht werden	♦ Archival data must be effectively deleted after the retention period has expired	☒	
♦ Keine Archivierung auf Datenträgern, die für eine lange Speicherdauer ungeeignet sind	♦ No archiving on data carriers that are unsuitable for a long storage period	☒	
♦ Keine Aufbewahrung von Archivdaten in Produktivdatenbanken, sondern Überspielen von Archivdaten aus Produktivsystemen in die Archivsysteme	♦ No storage of archive data in productive databases, but transfer of archive data from productive systems to the archive systems	☒	
♦ Eindeutige Verantwortlichkeiten für Löschungen festgelegt	♦ Clear responsibilities for deletions defined	☒	
♦ Einsatz von Aktenschreddern (mind. Sicherheitsstufe 3, cross cut)	♦ Use of document shredders (min. security level 3, cross cut)	☒	
♦ Physische Löschung von Datenträgern ("sicheres Löschen" durch ein- oder mehrmaliges Überschreiben mit speziellen Bit-	♦ Physical deletion of data carriers ("secure deletion" by overwriting once or several times with special bit combinations) or physical destruction of data carriers	☒	

Kombinationen) oder körperliche Vernichtung von Datenträgern				
♦ Protokollierung der externen Datenträgervernichtung	♦ Recording of the external destruction of data media	☒		

12. Wartung durch Dienstleister / Maintenance by service provider

Die Tätigkeiten von externen IT-Dienstleistern, insbesondere bei Wartung, müssen überwacht und dokumentiert werden. Um eine ungewollte Datenweitergabe zu verhindern, müssen personenbezogene Daten auf ausgemusterter Hardware sorgfältig gelöscht werden.	The activities of external IT service providers, especially during maintenance, must be monitored and documented. To prevent unwanted data disclosure, personal data on decommissioned hardware must be carefully deleted.

Wartung durch Dienstleister / Maintenance by service provider		durch	
		UN	DL
♦ Aufzeichnung aller Tätigkeiten von externen Dienstleistern	♦ Record of all activities of external service providers	☒	
♦ Verschwiegenheitsverpflichtung in den Dienstleistungsvertrag aufgenommen oder von dem externen Mitarbeiter unterzeichnet	♦ Confidentiality agreement included in the service contract or signed by the external service provider.	☒	
♦ Internen Mitarbeiter festlegen, der die Tätigkeiten des externen Dienstleisters überwacht (bzw. ggf. begleitet) und dokumentiert	♦ Appoint an internal employee to monitor (or, if necessary, accompany) and document the activities of the external service provider.	☒	
♦ Regelungen zur wirksamen Datenlöschung auf Hardware (z. B. PCs, Drucker, Smartphones) schaffen, die vom Dienstleister oder Hersteller zurückgenommen werden (z. B. bei Defekten, Abschreibung)	♦ Establish regulations for effective data deletion on hardware (e.g. PCs, printers, smartphones) that are taken back by the service provider or manufacturer (e.g. in case of defects, depreciation).	☒	
♦ Bei Einsatz von Fernwartungssoftware regelmäßig Sicherheitsupdates einspielen und auf Informationen über bekannte Schwachstellen oder Fehlkonfigurationen achten	♦ When using remote maintenance software, regularly install security updates and pay attention to information about known vulnerabilities or misconfigurations.	☒	
♦ Fernwartung externer Dienstleister protokollieren und den Zugang nur auf das zu wartende System begrenzen – sofern möglich, durch einen Mitarbeiter am Bildschirm des	♦ Log remote maintenance by external service providers and limit access only to the system to be maintained - if possible, track digitally by an employee on the screen of the maintained system	☒	

gewarteten Systems digital nachverfolgen		

13. Protokollierung / recording

Mittels geeigneter Protokollierungen können Sicherheitsverletzungen nach Art. 33 DS-GVO auch im Nachhinein erkannt und aufgearbeitet werden. Ohne Auflistung von Benutzeraktivitäten kann dagegen meist keine valide Bewertung stattfinden, ob und in welchem Umfang ein unbefugter Datenzugriff erfolgte.	By means of suitable logging, security breaches pursuant to Art. 33 of the GDPR can also be detected and processed retrospectively. Without a list of user activities, on the other hand, it is usually not possible to make a valid assessment of whether and to what extent unauthorised data access has occurred.

Protokollierung / recording		durch	
		UN	DL
♦ Die Uhren der verwendeten Informationsverarbeitungssysteme (PCs, Notebooks, etc.) sollten mit geeigneten Zeitquellen synchronisiert werden, um eine gezielte Analyse bei Sicherheitsereignissen zu ermöglichen	♦ The clocks of the information processing systems used (PCs, notebooks, etc.) should be synchronised with suitable time sources to enable targeted analysis in the event of security events	☒	
♦ Regelmäßige anlasslose Auswertung der Log-Dateien zur Erkennung von ungewöhnlichen Einträgen – bevorzugt: Automatische Heuristiken	♦ Regular evaluation of the log files without any reason in order to detect unusual entries - preferably: automatic heuristics	☒	

14. Business Continuity

Die Verfügbarkeit der Geschäftsprozesse und der damit verbundenen IT-Systeme und Daten ist zu gewährleisten. Im Rahmen des Backup-Konzepts ist daher ein geordnetes Zusammenspiel beim Wiedereinspielen gespeicherter Datenbestände wichtig, um im Notfall weiter betriebsfähig zu bleiben.	The availability of business processes and the associated IT systems and data must be guaranteed. Within the framework of the backup concept, it is therefore important to have an orderly interaction when restoring stored data stocks in order to remain operational in the event of an emergency.

Business Continuity		durch	
		UN	DL
♦ Durchführung von Backups nach der 3-2-1 Regel: 3 Datenspeicherungen, 2 verschiedene Backupmedien (auch	♦ Carry out backups according to the 3-2-1 rule: 3 data storages, 2 different backup media (also	☒	☒

„Offline“ wie Bandsicherungen) und 1 davon an einem externen Standort	"offline" like tape backups) and 1 of them at an external location.		
♦ Geeignete physische Aufbewahrung von Backupmedien (z. B. Tresor, unterschiedliche Brandabschnitte, Gefahr von Wasserschäden, ...)	♦ Suitable physical storage of backup media (e.g. safe, different fire compartments, risk of water damage, ...)	☒	
♦ Regelmäßige Überprüfung, ob mindestens ein Backup täglich durchgeführt wird	♦ Regular checks that at least one backup is carried out daily	☒	
♦ Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert	♦ Regular tests to ensure that all relevant data is included in the backup process and that the recovery works	☒	
♦ Mindestens ein Backup-System ist durch Schadcode nicht verschlüsselbar, z. B. spezielles Datensicherungsverfahren wie Pull-Verfahren des Backup-Systems oder Air-Gap- getrennt (offline) nach Abschluss des Backup-Prozesses	♦ At least one backup system cannot be encrypted by malicious code, e.g. special data backup procedure such as pull procedure of the backup system or air-gap separated (offline) after completion of the backup process	☒	
♦ Weitestgehender Verzicht auf Makros in Office-Dokumenten im Betriebsalltag zum Schutz vor Ransomware	♦ As far as possible, refrain from using macros in Office documents in everyday operations to protect against ransomware.	☒	
♦ Zulassen ausschließlich signierter Microsoft Office-Makros oder (regelmäßige) Information, bspw. einmal pro Jahr, der Beschäftigten über Risiken einer Makro-Aktivierung (z. B. in Microsoft Word)	♦ Allow only signed Microsoft Office macros or (regularly) inform employees, e.g. once a year, about the risks of macro activation (e.g. in Microsoft Word).	☒	
♦ Deaktivierung von Windows Script Hosts (WSH) auf Clients (sofern nicht zwingend benötigt) oder Prüfung, ob die Einschränkung von Powershell-Skripten mit dem „ConstrainedLanguage Mode“ auf Windows-Clients sinnvoll durchführbar ist oder Nutzen eines Web-Proxys mit (tages-)aktuellen Sperrlisten von Schadcode-Download-Seiten (IOCs)	♦ Deactivating Windows Script Hosts (WSH) on clients (if not absolutely necessary) or checking whether the restriction of Powershell scripts with the "ConstrainedLanguage Mode" on Windows clients is feasible or using a web proxy with (daily) current blocking lists of malicious code download sites (IOCs).	☒	

15. Kryptographie / Cryptography

Mittels kryptographischen Verfahren nach Stand der Technik kann die Vertraulichkeit, Integrität und Authentizität von Daten, Systemen und Entitäten sichergestellt werden	The confidentiality, integrity and authenticity of data, systems and entities can be ensured by means of state-of-the-art cryptographic procedures.

Kryptographie / Cryptography		durch	
		UN	DL
♦ Passwortspeicherung mit Salt nach Stand der Technik	♦ Password storage with Salt according to the state of the art	☒	
♦ Asymmetrische Verschlüsselung nach Stand der Technik mit B. RSA-2048 Bit (oder höher), EC-256 Bit (oder höher)	♦ State-of-the-art asymmetric encryption with B. RSA-2048 bit (or higher), EC-256 bit (or higher)	☒	
♦ Wirksame Schlüsselverwaltung (Generierung, Ausgabe, Sperrung) ist bei Einsatz kryptographischer Verfahren essenziell	♦ Effective key management (generation, issuance, blocking) is essential when using cryptographic methods	☒	
♦ Schutz von geheimen Schlüsseln durch starke Passwörter mit mindestens 16 Stellen. Bei hohem Risiko Einsatz von HSM (Hardware Security Modulen) prüfen	♦ Protection of secret keys by strong passwords with at least 16 digits. Check the use of HSM (hardware security modules) in the case of high risk.	☒	
♦ SSL-Zertifikate bei vertrauenswürdigen Zertifizierungsstellen beschaffen	♦ Procure SSL certificates from trustworthy certification authorities.	☒	
♦ HTTPS nach Stand der Technik (z. B. mind. 2048-Bit RSA, Perfect Forward Secrecy, HSTS, ggf. Client Zertifikate) einsetzen	♦ Use HTTPS according to the state of the art (e.g. at least 2048-bit RSA, Perfect Forward Secrecy, HSTS, client certificates if necessary).	☒	
♦ Keine kryptographischen Verfahren mit bekannten Schwachstellen oder zu kurzer Schlüssellänge mehr verwenden, z. B. DES, 3-DES, MD5, SHA-1	♦ No longer use cryptographic procedures with known vulnerabilities or too short a key length, e.g. DES, 3-DES, MD5, SHA-1	☒	

16. Datentransfer / data transfer

Sowohl der Datenaustausch mit anderen Stellen über elektronische Kommunikationsnetze als auch der physikalische Transport von mobilen Datenträgern und Dokumenten müssen derart abgesichert werden, dass die Vertraulichkeit und	Both the exchange of data with other bodies via electronic communication networks and the physical transport of mobile data carriers and documents must be secured in such a way that the confidentiality and integrity of personal data is not compromised.

Integrität der personenbezogenen Daten nicht beeinträchtigt wird.	

Datentransfer / data transfer		durch	
		UN	DL
♦ Regeln für alle Arten von Datentransfers sowohl innerhalb der Organisation als auch zwischen der Organisation und anderen Parteien bestehen	♦ Rules exist for all types of data transfers, both within the organisation and between the organisation and other parties.	☒	
♦ Verschlüsselung von mobilen Datenträgern (wie DVD, USB-Sticks, Festplatte) nach Stand der Technik	♦ Encryption of mobile data carriers (such as DVD, USB sticks, hard disk) according to the state of the art.	☒	
♦ Bei E-Mail, Cloud-Plattformen: Transportverschlüsselung von personenbezogenen Daten nach Stand der Technik bei normalem Risiko	♦ For e-mail, cloud platforms: Transport encryption of personal data according to the state of the art for normal risk.	☒	
♦ Bei E-Mail, Cloud-Plattformen: Transportverschlüsselung und Inhaltsverschlüsselung von personenbezogenen Daten nach Stand der Technik bei hohem Risiko	♦ For e-mail, cloud platforms: State-of-the-art transport encryption and content encryption of personal data in the event of high risk	☒	
♦ Bei Messenger: Transport- und Inhaltsverschlüsselung der Nachrichten und Dateien	♦ For messenger: transport and content encryption of messages and files	☒	
♦ Sicherstellung der Integrität von personenbezogenen Daten durch digitale Signaturen zumindest bei hohem Risiko	♦ Ensuring the integrity of personal data through digital signatures at least in the case of high risk	☒	
♦ Bei HTTPS: Einsatz von Client-Zertifikaten zum Nachweis der Authentizität bei geschlossenem Nutzerkreis	♦ For HTTPS: Use of client certificates to prove authenticity for a closed user group.	☒	

17. Entwicklung und Auswahl von Software / development and selection of software

Datenschutz und Sicherheit müssen frühzeitig bei der Entwicklung von eigenen Softwaresystemen bzw. bei der Auswahl von Softwareprodukten im eigenen Betrieb berücksichtigt werden.	Data protection and security must be taken into account at an early stage in the development of one's own software systems or in the selection of software products in one's own business.

Entwicklung und Auswahl von Software / development and selection of software		durch	
		UN	DL
♦ Relevante Mitarbeiter sind 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 (Produktauswahl, zentral vs. dezentral, Pseudonymisierung, Verschlüsselung, Land eines Dienstleisters) hat	♦ Relevant employees are trained that security-by-design (ensuring confidentiality, availability and integrity) as a subset of data protection-by-design is a legal data protection requirement and has an influence on central design decisions (product selection, central vs. decentralised, pseudonymisation, encryption, country of a service provider).	☒	
♦ Es findet eine Trennung von Produktivsystem zu Entwicklungs-/Testsystem statt	♦ There is a separation of productive system from development/test system	☒	
♦ Den Zugang zum Source-Code bei der Entwicklung von Software beschränken	♦ Restrict access to the source code when developing software	☒	
♦ Keine personenbezogenen Daten oder Zugangsdaten in der Source-Code-Verwaltung ablegen	♦ Do not store any personal data or access data in the source code management system	☒	
♦ System- und Sicherheitstests, wie z. B. Code-Scan	♦ System and security tests, e.g. code scan	☒	
♦ Datensätze sind mit Zweckattributen vesehen (z.B. Text- oder Zahlenfeld mit Namen, Größe oder auch Metadaten wie Keyword, Titel oder die H1Überschrift in einer HTML-Definition)	♦ Data records are marked with purpose attributes (e.g. text or number field with name, size or even metadata such as keyword, title or the H1 heading in an HTML definition)	☒	
♦ Festlegung von Datenbankrechten entsprechend dem Rollen-Rechtekonzept	♦ Definition of database rights according to the role rights concept	☒	
♦ Mandantenfähigkeit relevanter Anwendungen	♦ Multi-client capability of relevant applications	☒	
♦ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	♦ Physical separation (systems / databases / data carriers)	☒	
♦ Ausreichende Testzyklen werden berücksichtigt	♦ Sufficient test cycles are taken into account	☒	

♦ Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen	♦ Standard software and corresponding updates are only obtained from trustworthy sources	☒	
♦ Sicherstellung, dass ein fortlaufender Plan zur Überwachung, Bewertung und Anwendung von Updates oder Konfigurationsänderungen für die gesamte Lebenszeit einer Softwareanwendung besteht	♦ Ensuring that there is an ongoing plan for monitoring, evaluating and applying updates or configuration changes for the entire lifetime of a software application	☒	

18. Auftragsverarbeiter / processors

Dienstleister, die personenbezogene Daten im Rahmen einer Auftragsverarbeitung behandeln, benötigen geeignete Garantien, damit auch die Sicherheit der Verarbeitung gewährleistet werden kann.	Service providers who handle personal data as part of commissioned processing require appropriate guarantees so that the security of the processing can also be ensured.

Auftragsverarbeiter / processors		durch	
		UN	DL
♦ Nur Dienstleister verwenden, die die Garantien (in Form von Dokumenten) zur Verfügung stellen können	♦ Only use service providers who can provide the guarantees (in the form of documents).	☒	
♦ Sicherheitsmaßnahmen nach Art. 32 DS-GVO als Bestandteil eines AV-Vertrags müssen zur Dienstleistung passen – das Abstraktionsniveau der Maßnahmen ist mitunter leicht höher als bei internen TOM-Listen eines Verantwortlichen	♦ Security measures according to Art. 32 GDPR as part of an AV contract must fit the service - the level of abstraction of the measures is sometimes slightly higher than in the case of internal TOM lists of a data controller	☒	
♦ Die Wirksamkeit der Garantien kann durch geeignete Zertifizierungen (ansatzweise) nachgewiesen werden – Bsp.: ISO 27001 bei Rechenzentrum mit Scope Physikalische Sicherheit ist meist aussagekräftig	♦ The effectiveness of the guarantees can be proven (to some extent) by suitable certifications - e.g. ISO 27001 for a data centre with scope physical security is usually meaningful	☒	
♦ Eine Vor-Ort-Kontrolle durch den Verantwortlichen wird nicht ausgeschlossen werden	♦ An on-site inspection by the person responsible will not be excluded	☒	

♦ Der Auftragsverarbeiter darf keine weiteren Subdienstleister ohne Information des Auftraggebers aufnehmen – dieser hat dann ein Widerspruchsrecht	♦ The processor may not take on any further sub-service providers without informing the client - the client then has a right of objection	☒	
♦ Der Auftragsverarbeiter muss Prozesse bei der Erkennung von Datenschutzverletzungen haben und diese unverzüglich dem Verantwortlichen im Sinne der DS-GVO melden	♦ The processor must have processes in place to detect data protection breaches and report them immediately to the controller as defined by the GDPR	☒	
♦ Transfers in unsichere Drittländer sind ggf. nur mit weiteren technischen Schutzmaßnahmen, primär dem Einsatz von kryptographischen Verfahren, möglich	♦ Transfers to insecure third countries may only be possible with further technical protection measures, primarily the use of cryptographic procedures.	☒	
♦ Daten werden bei Auftragsverarbeitung (spätestens) nach Vertragsende wirksam gelöscht	♦ In the case of commissioned processing, data is effectively deleted (at the latest) after the end of the contract.	☒	
♦ Angaben zur Löschmethodik können bei Bedarf zur Verfügung gestellt werden	♦ - Details of the deletion method can be provided if required.		
♦ Regelmäßige Überprüfung des Auftragsverarbeiters bezüglich Sicherheitspraktiken und Dienstleistungserbringung	♦ Regular review of the processor with regard to security practices and service provision	☒	
♦ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen (z.B. in einem VVT)	♦ Documentation of data recipients as well as the duration of the planned transfer or deletion periods (e.g. in a VVT)	☒	
♦ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen (z.B. Postausgangsbuch, Outlook-, Thunderbirdverlauf)	♦ Overview of regular retrieval and transfer processes (e.g. outgoing mail book, Outlook, Thunderbird history)	☒	
♦ Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen	♦ Careful selection of transport staff and vehicles	☒	
♦ Persönliche Übergabe papiergebundener Dokumente mit Protokoll (z.B. Abholschein	♦ Personal handover of paper-based documents with protocol (e.g. pick-up slip for document	☒	

Aktenvernichter, Rückschein bei Einschreiben)	shredder, return receipt for registered mail)		
♦ Weitergabe in anonymisierter oder pseudonymisierter Form (z.B. für statistische Zwecke)	♦ Transfer in anonymised or pseudonymised form (e.g. for statistical purposes)	☒	
♦ Sichere Transportbehälter für papiergebundene Dokumente (z.B. Post-Container, verschließbare Daten-Mülltonnen)	♦ Secure transport containers for paper-based documents (e.g. post containers, lockable data waste bins)	☒	
♦ Regelmäßige Überprüfung des Auftragsverarbeiters bezüglich Sicherheitspraktiken und Dienstleistungserbringung	♦ Regular review of the processor with regard to security practices and service provision.	☒	
♦ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus	♦ In case of longer cooperation: Ongoing review of the Processor and its level of protection.	☒	
♦ Der Auftragsverarbeiter darf keine weiteren Subdienstleister ohne Information des Auftraggebers aufnehmen – dieser hat dann ein Widerspruchsrecht	♦ The processor must not take on any further sub-service providers without informing the client - the client then has a right of objection	☒	
♦ Der Auftragsverarbeiter muss Prozesse bei der Erkennung von Datenschutzverletzungen haben und diese unverzüglich dem Verantwortlichen im Sinne der DSGVO melden	♦ The processor must have processes in place to identify data protection breaches and report them immediately to the controller as defined by the GDPR.	☒	
♦ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis	♦ Obligation of the Processor's employees to maintain data confidentiality	☒	
♦ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht	♦ Obligation to appoint a data protection officer by the Processor if there is an obligation to appoint one	☒	

Ausgefüllt für die Organisation durch / Filled for the organization by

Name	Mark Henkel
Funktion/function	Geschäftsführung (CEO) und IT Service
Rufnummer / Phone.no.	03683-4661872

E-Mail mark.henkel@dsign-systems[at]de

Ort, Datum / Place/Date: Schmalkalden, 01.11.2022

Vom Prüfer auszufüllen:

Wiederholungsprüfung am 04.11.2022 durch Karsten Greibel (Date Protection Risk Manager (FOM), ICO CISIS12 Porfessional. Ergebnis(se): Nach dem ausführlichen Audit der Geschäftsstelle in Schmalkalden am 04.11.2022 durch den Data Protection Risk Manager (FOM) Karsten Greibel werden die oben aufgeführten technischen und organisatorischen Maßnahmen zur Sicherung personenbezogener Daten gemäß Artikel 32 EU-Datenschutzgrundverordnung bestätigt und testiert.	Re-Audited on 04.11.2022 by Karsten Greibel (Date Protection Risk Manager (FOM), ICO CISIS12 Porfessional. Result(s): Following the detailed audit of the Schmalkalden office on 04.11.2022 by the Data Protection Risk Manager (FOM) Karsten Greibel, the technical and organisational measures listed above to secure personal data in accordance with Article 32 of the EU General Data Protection Regulation are confirmed and attested.

☒ TOM sind für den angestrebten Schutzzweck ausreichend / TOM are sufficient for the intended protective purpose

☒ Vereinbarung Auftragsverarbeitung kann geschlossen werden / Commissioned processing privacy agreement can be concluded

Meiningen, 04.11.2022

Ort, Datum / Place,Date

X

Karsten Greibel
Data Protection Risk Manager (FOM)

Spezifizierte technische und organisatorische Sicherheitsmaßnahmen der WebAPP TaskCards® gemäß Art 32 Datenschutzgrundverordnung (DSGVO)

Specified technical and organisational security measures of the WebAPP TaskCards® in accordance with Art 32 of the General Data Protection Regulation (GDPR)

Die nachfolgenden Ausführungen beziehen sich in spezifizierter Weise auf die Datensicherheits- und Datenschutzeinstellungen der WebApp TaskCards auf den Servern unserer Dienstleister. Die aufgeführten Maßnahmen werden zusätzlich zu den allgemeinen technischen und organisatorischen Maßnahmen der DSign Systems GmbH mit Hilfe von ausgewählten Dienstleistern umgesetzt. Die Dokumente allgm_TOM_DSign und spez_TOM_WebApp_TaskCards stellen das vollständige Sicherheitskonzept der Anwendung dar.	The following statements refer in a specified manner to the data security and data protection settings of the WebApp TaskCards on the servers of our service providers. The measures listed are implemented in addition to the general technical and organisational measures of DSign Systems GmbH with the help of selected service providers. The documents allgm_TOM_DSign and spez_TOM_WebApp_TaskCards represent the complete security concept of the application.

1. Vertraulichkeit / Confidentiality (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle *Unbefugten wird der Zutritt zu Räumen, in denen die Datenverarbeitungs-anlagen untergebracht sind verwehrt.* Es werden folgende Maßnahmen umgesetzt: Festlegung von Sicherheitsbereichen, Realisierung eines wirksamen Zutrittsschutzes, Protokollierung des Zutritts, Festlegung Zutrittsberechtigter Personen, Verwaltung von personengebundenen Zutrittsberechtigungen, Begleitung von Fremdpersonal, Überwachung der Räume.	**Entry control** *Unauthorised persons are denied access to rooms in which the data processing equipment is housed.* The following measures are implemented: Definition of security areas, implementation of effective access protection, logging of access, definition of persons authorised to access, administration of personal access authorisations, escorting of external personnel, monitoring of rooms.

Zugangskontrolle *Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.* Es werden folgende Maßnahmen umgesetzt: Festlegung des Schutzbedarfs, Zugangsschutz, Umsetzung sicherer Zugangsverfahren, starke Authentisierung, Umsetzung einfacher Authentisierung per Username Passwort, Protokollierung des Zugangs, Monitoring bei kritischen IT-Systemen, Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen, Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen, Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients), Festlegung befugter Personen, Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen, Automatische Zugangssperre und Manuelle Zugangssperre.	**Access control** *Data processing systems shall be prevented from being used by unauthorised persons.* The following measures shall be implemented: Determination of the need for protection, access protection, implementation of secure access procedures, strong authentication, implementation of simple authentication via username password, logging of access, monitoring for critical IT systems, secured (encrypted) transmission of authentication secrets, blocking in case of failed attempts/activity and process for resetting blocked access IDs, prohibition of storage function for passwords and/or form entries (server/clients), determination of authorised persons, administration and documentation of person-bound authentication media and access authorisations, automatic access blocking and manual access blocking.
Zugriffskontrolle *Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.* Es werden folgende Maßnahmen umgesetzt: Erstellen eines Berechtigungskonzepts, Umsetzung von Zugriffsbeschränkungen, Vergabe minimaler Berechtigungen, Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen, Vermeidung der Konzentration von Funktionen	**Access management** *Only data for which access authorisation exists can be accessed. Data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.* The following measures are implemented: Creation of an authorisation concept, implementation of access restrictions, allocation of minimal authorisations, administration and documentation of personal access authorisations, avoidance of concentration of functions.
Verwendungszweckkontrolle *Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.* Es werden folgende Maßnahmen umgesetzt: Datensparsamkeit im Umgang mit personenbezogenen Daten, Getrennte Verarbeitung verschiedener Datensätze, Regelmäßige Verwendungszweck-kontrolle und Löschung, Trennung von Test- und Entwicklungsumgebung datenschutzfreundliche Voreinstellungen	**Purpose of use control** Ensure that data collected for different purposes can be processed separately. The following measures shall be implemented: Data economy in handling personal data, Separate processing of different data sets, Regular purpose of use control and deletion, Separation of test and development environment. Data protection-friendly default settings

Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, sind die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der Betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.	If data is not required to achieve the purpose of use, the technical default settings are defined in such a way that data is only collected, processed, passed on or published as a result of an action by the data subject.

2. Integrität / integrity (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle *Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.* Es werden folgende Maßnahmen umgesetzt: Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen, Protokollierung von Übermittlungen gemäß Protokollierungskonzept, Sichere Datenübertragung zwischen Server und Client (TLS1.2), Sicherung der Übertragung im Backend, Sichere Übertragung zu externen Systemen, Risikominimierung durch Netzseparierung, Implementation von Sicherheitsgateways an den Netzübergabepunkten, Härtung der Backendsysteme, Beschreibung der Schnittstellen, Umsetzung einer Maschine-Maschine-Authentisierung, Sichere Ablage von Daten, inkl. Backups, Gesicherte Speicherung auf mobilen Datenträgern, Einführung eines Prozesses zur Datenträgerverwaltungen, Prozess zur Sammlung und Entsorgung, Datenschutzgerechter Lösch- und Zerstörungsverfahren, Führung von Löschprotokollen	**Transfer Control** *The objective of the transfer control is to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.* The following measures shall be implemented: Definition of instances/persons authorised to receive/transmit, logging of transmissions according to the logging concept, secure data transmission between server and client (TLS1.2), securing of transmission in the backend, secure transmission to external systems, risk minimisation through network separation, implementation of security gateways at the network transfer points, hardening of the backend systems, description of the interfaces, implementation of machine-to-machine authentication, secure storage of data, incl. backups, secure storage on the server (TLS1.2). backups, secure storage on mobile data media, implementation of a process for data media management, process for collection and disposal, data protection-compliant deletion and destruction procedures, maintenance of deletion logs
Eingabekontrolle *Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in*	**Input control** *The purpose of input control is to ensure that it can be subsequently verified and determined whether and by*

Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Es werden folgende Maßnahmen umgesetzt: Protokollierung der Eingaben, Dokumentation der Eingabeberechtigungen	*whom personal data have been entered into, modified or removed from data processing systems.* The following measures are implemented: logging of inputs, documentation of input authorisations

3. Verfügbarkeit, Belastbarkeit, Desaster Recovery / availability, resilience, disaster recovery

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) Es werden folgende Maßnahmen umgesetzt: Brandschutz, Redundanz der Primärtechnik, Redundanz der Stromversorgung, Redundanz der Kommunikationsverbindungen, Monitoring, Resourcenplanung und Bereitstellung, Abwehr von systembelastendem Missbrauch, Datensicherungskonzepte und Umsetzung, Regelmäßige Prüfung der Notfalleinrichtungen **Desaster Recovery - Rasche Wiederherstellung nach Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)** Es werden folgende Maßnahmen umgesetzt: Notfallplan, Datensicherungskonzepte und Umsetzung	**Availability and resilience (Art. 32 para. 1 lit. b GDPR).** The following measures are implemented: Fire protection, redundancy of primary technology, redundancy of power supply, redundancy of communication links, monitoring, resource planning and provisioning, defence against system-impacting misuse, data backup concepts and implementation, regular testing of emergency facilities. **Disaster recovery - rapid recovery after an incident (Art. 32 Para. 1 lit. c GDPR)** The following measures are implemented: Emergency plan, data backup concepts and implementation

4. Datenschutzorganisation der Hostinanbieter / data protection organisation of the host providers

Unsere eingesetzten Hostinganbieter haben aufgrund Ihrer Zertifizierungen ein eigenständiges Datenschutzmanagementsystem. Das System umfasst u.a.: Festlegung von Verantwortlichkeiten, Umsetzung und Kontrolle geeigneter Prozesse, Melde- und Freigabeprozess, Umsetzung von Schulungsmaßnahmen, Verpflichtung der	Our hosting providers have an independent data protection management system due to their certifications. The system includes, among other things: Definition of responsibilities, implementation and control of suitable processes, reporting and approval process, implementation of training measures, obligation of employees and service

Mitarbeiter und Dienstleister auf Vertraulichkeit, Regelungen zur internen Aufgabenverteilung, Beachtung von Funktionstrennung und -zuordnung, Einführung einer geeigneten Vertreterregelung	providers to confidentiality, regulations on the internal distribution of tasks, observance of the separation and allocation of functions, introduction of a suitable deputy regulation.

5. Auftragskontrolle / processor controlls

Die TaskCards WebAPP stellt eine Software as a Service (SaaS)-Lösung dar. Die TaskCards WebAPP wird daher auf den Servern von ausgewählten Hosting-Anbietern gehostet, um jederzeit eine zuverlässige, sichere und schnelle Verfügbarkeit aller Daten und Inhalte auf den unterstützen Endgeräten zu gewährleisten. Neben dem Front- und Backend der TaskCards WebAPP werden auf diesen Servern auch sämtliche in der TaskCards WebAPP verarbeitete Daten sowie Backups gespeichert. Erfasst sind insbesondere auch die im Auftragsverarbeitungsvertrag benannten personenbezogenen Daten.	The TaskCards WebAPP represents a Software as a Service (SaaS) solution. The TaskCards WebAPP is therefore hosted on the servers of selected hosting providers to ensure reliable, secure and fast availability of all data and content on the supported end devices at all times. In addition to the front and back end of TaskCards WebAPP, all data processed in TaskCards WebAPP as well as backups are also stored on these servers. In particular, the personal data specified in the order processing contract is also recorded.
Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen von DSign Systems GmbH verarbeitet werden können. Die Auswahl der Hostinganbieter erfolgt ausschließlich unter Berücksichtigung geeigneter Garantien. Vor Inanspruchnahme der Dienstleistungen wurden die entsprechenden Abschlüsse von Vereinbarung zur Auftragsverarbeitung geschlossen. Als Hostinanbieter werden eingesetzt: • STRATO AG, Pascalstraße 10, 10587 Berlin • OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken Teil der Unternehmensgruppe OVH SAS-Gruppe, eine unter der Nummer 537 407 926 eingetragene Gesellschaft im Handels- und Gesellschaftsregister von Lille mit Sitz in 2, Rue Kellermann, 59100 Roubaix	The aim of the order control is to ensure that personal data processed on behalf can only be processed in accordance with the instructions of DSign Systems GmbH. The selection of hosting providers is carried out exclusively under consideration of appropriate guarantees. Prior to using the services, the relevant contract processing agreements have been concluded. The hosting providers used are: • STRATO AG, Pascalstraße 10, 10587 Berlin, Germany. • OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken Part of the OVH SAS Group, a company registered under number 537 407 926 in the Commercial and Companies Register of Lille, with its registered office at 2, Rue Kellermann, 59100 Roubaix.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung / procedures for regular review, assessment and evaluation (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Die ausgewählten Hostinganbieter besitzen gültige Zertifikate u.a. Informationssicherheitsmanagement nach ISO 27001, weiterhin sind Prozesse zur Evaluation der Technischen und organisatorischen Maßnahmen und zum Sicherheitsvorfall-Management bei den Dienstleistern implementiert. Eine regelmäßige Durchführung von technischen Überprüfungen wird in diesem Zusammenhang geleistet. Die Standorte der Hostinganbieter bzw. deren Rechenzentren sind ausschließlich im europäischen Wirtschaftsraum.	The selected hosting providers have valid certificates, including information security management according to ISO 27001; furthermore, processes for the evaluation of technical and organisational measures and for security incident management are implemented at the service providers. Regular technical audits are carried out in this context. The locations of the hosting providers and their data centres are exclusively in the European Economic Area.

Name / Anschrift **Name / Address**	**Ort der Verarbeitung** **Place of processing**	**Zertifizierungen** **Certifications**	**Informationen zur IT-Sicherheit** **Information on IT-security**
STRATO AG, Pascalstraße 10, 10587 Berlin	Deutschland	ISO/IEC 27001:2013	STRATO-Sicherheitskonzept STRATO- *Security concept*
OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken Teil der Unternehmens-gruppe OVH SAS-Gruppe [...]Part of the OVH SAS Group	Deutschland, Frankreich / ausschließlich EWR zur Redundanten Speicherung und Sicherstellung der Backup-Strategie *Germany, France / exclusively EEA for redundant storage and ensuring the backup strategy*	ISO/IEC 27001:2013 ISO/IEC 27001 SOC 1, 2, 3 ANSSI SecNumCloud PCI DSS Level 1 C5 Katalog BSI	OVHcloud Sicherheitspolitik *OVHcloud Security Policy*