# Informationssicherheits- und Datenschutzkonzept

# der WebAPP Anwendung TaskCards®

Stand 20.11.2021


Inhalt:

## Einleitung

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.

## Erläuterung

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.

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.

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

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

# Testat zur Sicherheit der Verarbeitung

# gemäß Art. 32 Datenschutz-Grundverordnung (DSGVO)

Stand 19.11.2021

## Einleitung

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 der Verantwortliche 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.

Das Testat wird ausgestellt für das Unternehmen

dSign Systems GmbH
Waldhausstraße 14
98574 Schmalkalden

Das Testat berücksichtigt die am Unternehmensstandort umgesetzten Sicherheitsmaßnahmen.
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.

Das Unternehmen gewährleistet gemäß Art. 32 DSGVO folgende allgemeine, technischen und organisatorischen Sicherungsmaßnahmen:

## 1. Management und 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.

| | 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 | ☒ | |
| ♦ Die Rollen der einzelnen Mitarbeiter im Sicherheitsprozess sind eindeutig festgelegt | ☒ | |
| ♦ Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach dem PDCA-Zyklus | ☒ | |
| ♦ Konzepte und Dokumentationen im Sicherheitsumfeld werden regelmäßig überprüft und aktuell gehalten | ☒ | |
| ♦ Je nach Unternehmensgröße: Einsatz eines geeigneten Informationssicherheits-managementsystem (ISMS), z. B. nach ISO/IEC 27001, BSI-Standards oder CISIS12 | ☒ | |
| ♦ Die Rollen und Verantwortlichkeiten im Bereich der Sicherheit sind im eigenen Betrieb bekannt und besetzt (u. a. Informationssicherheitsbeauftragter (ISB), IT-Leiter, Datenschutzbeauftragter (DSB)) | ☒ | |
| ♦ Konsequente Einbindung des DSB bei Sicherheitsfragen | ☒ | |
| ♦ Ein Datenschutzbeauftragter ist offiziell benannt und gemeldet | ☒ | |
| ♦ Ein Informationssicherheitsbeauftragter ist benannt | ☒ | |
| ♦ Mitarbeiter sind der Verschwiegenheit schriftlich verpflichtet | ☒ | |
| ♦ Ausreichende fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema | ☒ | |
| ♦ Ausreichende fachliche Qualifikation des ISB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema | ☒ | |
| ♦ Durchführung von regelmäßigen Audits des DSB nach Art. 32 DS-GVO zur Sicherheit der Verarbeitung | ☒ | |
| ♦ Durchführung von regelmäßigen internen Audits des ISB zur Sicherheit der Verarbeitung | ☒ | |
| ♦ Kenntnis der zuständigen Datenschutzaufsichtsbehörde sowie Wissen über die Meldeverpflichtungen nach Art. 33 und 34 DS-GVO (Verletzung der Sicherheit) | ☒ | |
| ♦ Aktive Unterstützung der Zusammenarbeit des DSB mit dem ISB durch die Unternehmensleitung | ☒ | |
| ♦ Erkenntnisse über (neue) digitale Bedrohungen sind zu sammeln und potenzielle Auswirkungen auf den eigenen Betrieb abzuleiten | ☒ | |

## 2. Physikalische Sicherheit der Infrastruktur

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.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Es besteht ein Konzept zu Zutrittsregelungen und zur physischen Zugangskontrolle (Perimeterschutz) | ☒ | |
| ♦ Klare Regelungen zum Umgang mit Besuchern (z. B. Begleitung, Sicherheitszonen, Besucherausweise, Protokollierung, Zuständiger Mitarbeiter für Besucher) als Bestandteil des Konzeptes | ☒ | |
| ♦ Gelebte Regelungen zum Umgang auch mit externen Dienstleistern (z. B. bei Werkverträgen, Handwerker, Wartung von Systemen) – wie Verschwiegenheitserklärung, persönliche Begleitung in Sicherheitszonen oder Protokollierung | ☒ | |
| ♦ Schaffung von verschiedenen Sicherheitszonen (z. B. Besucherbesprechungen, Serverräume, Arbeitsplätze, Forschungsbereich) | ☒ | |
| ♦ Sichere Schließsysteme samt dokumentierter Schlüsselverwaltung | ☒ | |
| ♦ Das Gebäude (z. B. Wände, Fenster) und die Infrastruktur (z. B. Leitungen, Gefahrenmeldeanlagen) werden regelmäßig geprüft und gewartet | ☒ | |
| ♦ Umzäunung des Betriebsgeländes | ☒ | |
| ♦ Ausreichende Klimatisierung von Serverräumen | ☒ | |
| ♦ Einsatz von Anlagen zur Sicherstellung der Stromversorgung von Serversystemen (unterbrechungsfreie Stromversorgung (USV)), insbesondere bei kurzfristigen Stromausfällen oder Schwankungen | ☒ | |
| ♦ Absicherung der Gebäudeschächte (z.B. Lichtschächte vor Kellerfenstern) | ☒ | |
| ♦ Türen in sensiblen Bereichen mit Knauf an der Außenseite | ☒ | |
| ♦ Vergitterung der Fenster im EG | ☒ | |
| ♦ Risiken durch Überflutung/Starkregen prüfen, insbesondere bei Serverräumen im Keller oder anderen gefährdeten Bereichen | ☒ | |
| ♦ Sorgfalt bei Auswahl der Reinigungsdienste | ☒ | |

## 3. Awareness der Mitarbeiter

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.

| **Technische Maßnahmen** | durch | |
|---|---|---|
| | UN | DL |
| ♦ Das gesamte Personal der Organisation sollte eine angemessene Schulung für Informationssicherheit und Datenschutz erhalten, soweit dies für die jeweilige Funktion relevant ist, | ☒ | |

| | | |
|---|---|---|
| ♦ Anleitung „Manuelle Desktopsperre“ ist den Mitarbeitern bekannt und wird angewendet | ☒ | |
| ♦ Datenschutz- und Informationssicherheitsschulungen für neue Beschäftigte zeitnah nach Aufnahme des Beschäftigungsverhältnisses | ☒ | |
| ♦ Regelmäßige Auffrischungsschulungen für bestehendes Personal (mdst. einmal pro Jahr) | ☒ | |
| ♦ Regelmäßige Informationen im Betrieb an alle über Neuigkeiten zum Datenschutz und der IT-Sicherheit (z. B. per Mail, Intranet, Kollaborationsplattform, Aushang) | ☒ | |
| ♦ Schulungsinhalte: Beschäftigten lernen kennen, wie Cyberangriffe mittels Social-Engineerings eingeleitet werden (Hilfe zur Selbsthilfe) | ☒ | |
| ♦ Schulungsinhalte: Beschäftigten erfahren von den Gefahren der E-Mail-Kommunikation, insbesondere bei verschlüsselten E-Mail-Anhängen (z. B. Zip-Datei mit Passwort) | ☒ | |
| ♦ Schulungsinhalte: Beschäftigten erkennen gefälschte E-Mails (z. B. Absenderadressen, Auffälligkeiten, eingebettete 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) | ☒ | |
| ♦ Von Heimarbeit betroffenen Mitarbeiter werden die sichere Nutzung von „Homeoffice“ (Mobiles Arbeiten) Lösungen erläutert und spezifische Gefahren aufgezeigt | ☒ | |

## 4. Authentifizierung

Digitale Zugangsbeschränkungen helfen im Alltag.
Nutzer von IT-Systemen und Diensten müssen daher Ihre Zugangsberechtigung mit geeigneten Mitteln nachweisen.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Einweisung aller Mitarbeiter in den Umgang mit Authentifizierungsverfahren und -mechanismen | ☒ | |
| ♦ Vergabe von eindeutigen Kennungen für jeden Nutzer Vermeidung von Gruppenkennungen | ☒ | |
| ♦ 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 | ☒ | |
| ♦ Möglichst automatische Umsetzung der Passwortrichtlinie für starke Passwörter in den Systemen mit Nutzerkennungen | ☒ | |
| ♦ Verhinderung der Auswahl schwacher Passwörter bei Anwendungen (z. B. über Richtlinien oder technisch erzwungen über das 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) | ☒ | |
| ♦ Passwörter werden nach einem Sicherheitsvorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden | ☒ | |

| | | |
|---|---|---|
| ♦ 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 | ☒ | |
| ♦ 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 | ☒ | |
| ♦ Unterrichtung der Beschäftigten, dass Passwörter nicht auf Zettel oder Pinnwänden aufgezeichnet werden dürfen | ☒ | |
| ♦ Keine Speicherung von Passwörtern im Browser ohne Sicherung durch ein Masterpasswort | ☒ | |
| ♦ Keine Mehrfachverwendung eines Passworts für verschiedene Dienste, sofern kein zentrales Identitätsmanagement (z. B. Active Directory) verwendet wird | ☒ | |
| ♦ Für lokale Admin-Konten besonders starke Passwörter (z. B. mind. 16-stellig, komplex und ohne übliche Wortbestandteile sowie unterschiedlich für jeden 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) | ☒ | |
| ♦ Zeitverzögerung zwischen einzelnen Login-Versuchen (insbesondere bei über das Internet erreichbaren Anwendungen) zur Erschwerung von automatischen Online-Angriffen | ☒ | |
| ♦ Darstellung der Anzahl der fehlgeschlagenen Logins für einen Nutzer, der sich erfolgreich anmeldet. Ziel: Transparenz für stattgefundene Angriffe bzw. Angriffsversuche schaffen. | ☒ | |
| ♦ Passwörter nicht im Klartext speichern, sondern geeignete kryptographische Verfahren einsetzen (z. B. bcrypt mit Salt) | ☒ | |
| ♦ Regelungen zum automatischen Sperren von Passwörtern nach einem Sicherheitsvorfall treffen (z. B. Passwort-Hash so abändern, dass kein Klartextpasswort dazu besteht) | ☒ | |
| ♦ Standard-Authentifizierungsinformationen durch Hersteller bei Software werden nach der Installation geändert | ☒ | |

## 5. Rollen-/Rechtekonzept

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.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Erstellen von Rollenprofilen für die Beschäftigten unter Einbeziehung der Einträge des Verzeichnisses der Verarbeitungstätigkeiten | ☒ | |
| ♦ Regelungen zur Verwaltung der Rollen (Zuweisung, Entzug) an die Mitarbeiter etablieren | ☒ | |
| ♦ 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 | ☒ | |
| ♦ Verwaltung Benutzerrechte ausschließlich durch Administratoren | ☒ | |

| | | |
|---|---|---|
| ♦ Keine Administratorkennungen für Nutzer, die keine administrativen Tätigkeiten ausführen | ☒ | |
| ♦ Verschiedene administrative Rollen (z. B. Anlage neuer Benutzer, Durchführung von Backups, Konfiguration der Firewall) für die IT-Administration erstellen | ☒ | |
| ♦ Die Nutzung von Superuser (z. B. root unter Linux) soweit möglich nicht verwenden | ☒ | |
| ♦ Für Beschäftigte mit IT-Administrationsaufgaben zwei Benutzerkennungen einrichten: eine Administrationskennung und eine normale Nutzerkennung (für nicht-administrative Zwecke wie z. B. das Surfen im 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.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Eine Geräteverwaltung (Wer setzt welche Geräte in welchem Bereich ein?) ist vorhanden | ☒ | |
| ♦ Automatisches Sperren nach einer gewissen Zeitspanne der Inaktivität, falls manuelles Sperren bei Verlassen des Einflussbereichs nicht gewährleistet werden kann | ☒ | |
| ♦ Aktivierung einer Firewall, die unerwünschte Servicedienste auf dem Endgerät blockiert (z. B. versehentlich installierter Webserver) | ☒ | |
| ♦ Verwendung einer Anti-Viren-Lösung bzw. eines EndpointProtection-Systems mit regelmäßigen, mindestens tagesaktuellen Signatur-Updates und Regelungen, wie im Falle einer Warnmeldung zu verfahren ist | ☒ | |
| ♦ Zentrale Erfassung von Schadcode-Alarmmeldungen durch die IT-Administration | ☒ | |
| ♦ Konzept zum Patch Management vorhanden (u. a. UpdatePlan mit Übersicht der eingesetzten Software) | ☒ | |
| ♦ Regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software und Fachanwendungen (z. B. durch E-Mail Newsletter, Herstellerveröffentlichungen, Fachmedien, Sicherheitswarnungen) | ☒ | |
| ♦ Automatisches Einspielen von Sicherheitsupdates des Betriebssystems, der installierten Software (z. B. PDF-Reader) oder von Softwarebibliotheken (z. B. Java), sofern möglich | ☒ | |
| ♦ Personenbezogene Daten werden auf einem Speichermedium gespeichert werden, das von dem Backup erfasst wird (z. B. Netzlaufwerk) | ☒ | |
| ♦ Einbindung von externen Geräten durch technische Maßnahmen auf das erforderliche Mindestmaß begrenzen (z. B. bei USB-Sticks, Smartphones, externe Festplatten) | ☒ | |
| ♦ Fernwartung für Clients zu IT-Administrationszwecken ausschließlich über verschlüsselte Verbindungen nach Authentifizierung durch den Administrator und Freigabe durch den Nutzer | ☒ | |

| | | |
|---|---|---|
| ♦ Nur Betriebssysteme und Software einsetzen, für die noch Sicherheitsupdates zeitnah zur Verfügung gestellt werden | ☒ | |
| ♦ Gehäuseverriegelung an Serverschränken, um unbefugten Zugriff auf Speichermedien zu verhindern | ☒ | |
| ♦ 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) | ☒ | |
| ♦ Anwendungen werden an den Endgeräten möglichst ohne Administratorrechte auszuführen | ☒ | |
| ♦ Prozess zur wirksamen Datenlöschung vor Vergabe eines Endgeräts an einen anderen Mitarbeiter aufsetzen | ☒ | |
| ♦ 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) | ☒ | |

## 7. Mobile Datenspeicher

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.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Einsatz starker Verschlüsselung der mobilen Endgeräte (z. B. Festplattenverschlüsselung, Container-Lösungen) | ☒ | |
| ♦ Einsatz von Backup- und Synchronisierungsmechanismen zur Verhinderung eines größeren Datenverlusts bei Verlust und Diebstahl | ☒ | |
| ♦ Bei Smartphones: Zugang ausschließlich nach Authentifizierung (z. B. PIN, Passwort) – Länge der Kennung in Abhängigkeit von automatischen Sperr- und Löschfunktionen | ☒ | |
| ♦ 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 | ☒ | |
| ♦ Bei Smartphones: Cloud-Speicher für Datenbackup erst nach sorgfältiger Prüfung der datenschutzrechtlichen Anforderungen einsetzen (auch Beschäftigtendatenschutz bei „Find my Phone"-Funktionen) | ☒ | |
| ♦ Bei Smartphones: Nur sichere Quellen werden für die Installation von Apps verwendet. Apps werden vorher getestet und freigegeben | ☒ | |
| ♦ 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. Anbringung von verschließbaren Stahlkabeln) für Notebooks bei Bedarf zur Verfügung stellen | ☒ | |
| ♦ Regelungen zur Privatnutzung bei Notebooks und Smartphones geschaffen - Keine Privatnutzung | ☒ | |

| | | |
|---|---|---|
| ♦ Die Mitarbeiter kennen die Regelungen bei Verlust eines mobilen Endgerätes, z. B. Verlustmeldung beim Unternehmen und/oder Polizei | ☒ | |

## 8. Serversysteme

Serversysteme müssen mit besonderer Sorgfalt abgesichert werden, da Sicherheitsverletzungen dort i. d. R. aufgrund der großen Menge personenbezogener Daten enorme Auswirkungen haben können.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Nur kompetent geschulte Personen dürfen Administrationstätigkeiten auf den Servern durchführen | ☒ | |
| ♦ Verschiedene Administrationsrollen mit Rechten nach dem Least-Privileg-Prinzip für unterschiedliche Administrationsaufgaben (z. B. Softwareupdates, Konfiguration, Backup) einsetzen | ☒ | |
| ♦ Geregelter Prozess zum zeitnahen Einspielen von Sicherheitsupdates der Server – kritische Updates müssen unverzüglich eingespielt werden | ☒ | |
| ♦ Deaktivierung/Deinstallation von Standard Server-Diensten, die nicht benötigt werden (z. B. Webserver, Printserver) | ☒ | |
| ♦ Serverlokale Dienste über Firewall auf Servern vor Außenzugriff blockieren | ☒ | |
| ♦ Weitere Härtungsmaßnahmen für das eingesetzte Serverbetriebssystem prüfen | ☒ | |
| ♦ Serverraumüberwachung mit Sensoren für Temperatur und Feuchtigkeit | ☒ | |
| ♦ Verwendung von Schutzsteckdosen im Serverraum mit Überspannungsschutz | ☒ | |
| ♦ Installation RAID System / Festplattenspiegelung werden regelmäßig durchgeführt | ☒ | |
| ♦ Keine sanitären Anschlüsse im oder oberhalb des Archivs | ☒ | |
| ♦ Brandschutztüren insbesondere vor den sensiblen Bereichen | ☒ | |

## 9. Websites und Webanwendungen

Webseiten und Webanwendungen stellen meist leicht zugängliche Plattformen für Angriffe dar, die mit bekannten Best-Practice-Ansätzen meist gut abgesichert werden können.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Verwendung des HTTPS-Protokolls nach Stand der Technik (TLS1.2 oder TLS1.3) | ☒ | |
| ♦ Absicherung von Datenbanken auf dem Webserver mittels Firewalls | ☒ | ☒ |
| ♦ Fernzugang zu Webservern nur mit verschlüsselter Verbindung und Zwei-Faktor-Authentifizierung (z. B. SSH mit Client-Zertifikaten) | | ☒ |

| | | |
|---|---|---|
| ♦ Limitierung von Administrationsbereichen der Webanwendungen auf bestimmte IP-Adressen (z. B. Unternehmens- Gateway) | ☒ | |
| ♦ Nur geschulte bzw. kompetente Personen dürfen Administrationstätigkeiten auf den Servern durchführen | ☒ | |
| ♦ Geregelter Prozess zur Information über Sicherheitsupdates und zeitnahes Einspielen derselben, insbesondere bei gängigen Content-Management-Systemen (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 | | ☒ |
| ♦ Trennung von Webserver, Anwendungslogik und Datenhaltung einer Webanwendung durch eigene Server, die in eine geeignete Firewall-Architektur eingebunden sind | ☒ | |
| ♦ Sperrung der Auffindung von Inhalten durch Suchmaschinen (über robots.txt), sofern diese Inhalte nicht durch eine Suchmaschine gefunden werden sollen, | ☒ | |

## 10. Netzwerk

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.

| **Technische Maßnahmen** | durch | |
|---|---|---|
| | UN | DL |
| ♦ Geeignete Netzwerksegmentierung durchführen: Restriktive (physikalische) Trennung sensitiver Netze von Verwaltungsnetzen (mittels Firewall-Systemen) | ☒ | |
| ♦ Einsatz einer Firewall am zentralen Internetübergang | ☒ | ☒ |
| ♦ Blockierung aller nicht benötigten Dienste (z. B. 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) - Gängig: Konzept einer DMZ (Demilitarisierten Zone) | ☒ | |
| ♦ 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) | ☒ | |
| ♦ Nutzung eines WLAN-Gastzugang ohne Zugangsmöglichkeit zum internen Netzwerk | ☒ | |
| ♦ Protokollierungen auf Firewall-Ebene, um auch unbefugte Zugriffe zwischen den Netzen festzustellen und zu analysieren | ☒ | |
| ♦ Automatische Benachrichtigungen an die IT-Administration bei Verdacht auf unbefugte Verarbeitungen | ☒ | |
| ♦ Regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall (z. B. mittels Portscans auf die eigenen IP-Adressen von extern und periodischer Pentests) | ☒ | |

| | | |
|---|---|---|
| ♦ Einsatz von ausreichend qualifiziertem Personal/Dienstleister zur Konfiguration der Firewall | ☒ | ☒ |
| ♦ Prüfung eingehender E-Mails mittels Anti-Malwareschutz | ☒ | |
| ♦ Blockieren von gefährlichen Email-Anhängen (z. B. .exe, .doc, .cmd) | ☒ | |
| ♦ Einsatz von Intrusion-Detection-Systemen (IDS) oder Intrusion-Prevention-Systemen (IPS) | ☒ | |
| ♦ Anbindung von Niederlassungen oder Homeoffice über stark verschlüsselte VPN-Verbindungen mit Client-Zertifikatsauthentifizierung | ☒ | |

## 11. Archivierung

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.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Regelungen etabliert, welche Daten auf welcher Rechtsgrundlage aufbewahrt werden müssen und wie lange die Aufbewahrungsfrist ist | ☒ | |
| ♦ Zugänge zu den Archivdateien festlegen: Dokumentieren, Umsetzen und Prüfen | ☒ | |
| ♦ Archivdaten müssen nach Ablauf der Aufbewahrungsfrist wirksam gelöscht werden | ☒ | |
| ♦ Keine Archivierung auf Datenträgern, die für eine lange Speicherdauer ungeeignet sind (z. B. wiederbeschreibbare DVDs) | ☒ | |
| ♦ Keine Aufbewahrung von Archivdaten in Produktivdatenbanken, sondern Überspielen von Archivdaten aus Produktivsystemen in die Archivsysteme | ☒ | |
| ♦ Verschlüsselung von Archivdateien mit geeignetem Schlüsselmanagement: Entschlüsselungsschlüssel an mind. Zwei (örtlich) getrennten Stellen aufbewahren | ☒ | |
| ♦ Eindeutige Verantwortlichkeiten für Löschungen festgelegt | ☒ | |
| ♦ Einsatz von Aktenschreddern (mind. Sicherheitsstufe 3, cross cut) | ☒ | |
| ♦ Physische Löschung von Datenträgern ("sicheres Löschen" durch ein- oder mehrmaliges Überschreiben mit speziellen Bit-Kombinationen) oder körperliche Vernichtung von Datenträgern | ☒ | |
| ♦ Protokollierung der externen Datenträgervernichtung | ☒ | |

## 12. Wartung durch Dienstleister

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.

| | durch | |
|---|---|---|
| | UN | DL |
| • Aufzeichnung aller Tätigkeiten von externen Dienstleistern | ☒ | |
| • Verschwiegenheitsverpflichtung in den Dienstleistungsvertrag aufgenommen oder von dem externen Mitarbeiter unterzeichnet | ☒ | |
| • Internen Mitarbeiter festlegen, der die Tätigkeiten des externen Dienstleisters überwacht (bzw. ggf. begleitet) und dokumentiert | ☒ | |
| • Regelungen zur wirksamen Datenlöschung auf Hardware (z. B. PCs, Drucker, Smartphones) schaffen, die vom Dienstleister oder Hersteller zurückgenommen werden (z. B. bei Defekten, Abschreibung) | ☒ | |
| • Bei Einsatz von Fernwartungssoftware regelmäßig Sicherheitsupdates einspielen und auf Informationen über bekannte Schwachstellen oder Fehlkonfigurationen achten | ☒ | |
| • Fernwartung externer Dienstleister protokollieren und den Zugang nur auf das zu wartende System begrenzen – sofern möglich, durch einen Mitarbeiter am Bildschirm des gewarteten Systems digital nachverfolgen | ☒ | |

## 13. Protokollierung

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.

| | 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 | ☒ | |
| ♦ Regelmäßige anlasslose Auswertung der Log-Dateien zur Erkennung von ungewöhnlichen Einträgen – bevorzugt: Automatische Heuristiken | ☒ | |

## 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.

| | durch | |
|---|---|---|
| | UN | DL |

| | | |
|---|---|---|
| ♦ Durchführung von Backups nach der 3-2-1 Regel: 3 Datenspeicherungen, 2 verschiedene Backupmedien (auch „Offline“ wie Bandsicherungen) und 1 davon an einem externen Standort | ☒ | ☒ |
| ♦ Geeignete physische Aufbewahrung von Backupmedien (z. B. Tresor, unterschiedliche Brandabschnitte, Gefahr von Wasserschäden, …) | ☒ | |
| ♦ Regelmäßige Überprüfung, ob mindestens ein Backup täglich durchgeführt wird | ☒ | |
| ♦ Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert | ☒ | |
| ♦ 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 | ☒ | |
| ♦ Weitestgehender Verzicht auf Makros in Office-Dokumenten im Betriebsalltag zum Schutz vor 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) | ☒ | |
| ♦ 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) | ☒ | |

## 15. Kryptographie

Mittels kryptographischen Verfahren nach Stand der Technik kann die Vertraulichkeit, Integrität und Authentizität von Daten, Systemen und Entitäten sichergestellt werden.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Passwortspeicherung mit Salt nach Stand der Technik | ☒ | |
| ♦ Asymmetrische Verschlüsselung nach Stand der Technik mit B. RSA-2048 Bit (oder höher), EC-256 Bit (oder höher) | ☒ | |
| ♦ Wirksame Schlüsselverwaltung (Generierung, Ausgabe, Sperrung) ist bei Einsatz kryptographischer Verfahren essenziell | ☒ | |
| ♦ Schutz von geheimen Schlüsseln durch starke Passwörter mit mindestens 16 Stellen. Bei hohem Risiko Einsatz von HSM (Hardware Security Modulen) prüfen | ☒ | |
| ♦ SSL-Zertifikate bei vertrauenswürdigen Zertifizierungsstellen beschaffen | ☒ | |
| ♦ HTTPS nach Stand der Technik (z. B. mind. 2048-Bit RSA, Perfect Forward Secrecy, HSTS, ggf. Client Zertifikate) einsetzen | ☒ | |
| ♦ Es werden keine kryptographischen Verfahren mit bekannten Schwachstellen oder zu kurzer Schlüssellänge mehr verwendet, z. B. DES, 3-DES, MD5, SHA-1 – falls Altsystem diese noch erfordern, wird eine individuelle Risikoanalyse durchzuführen | ☒ | |

## 16. Datentransfer

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 Integrität der personenbezogenen Daten nicht beeinträchtigt wird.

.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Regeln für alle Arten von Datentransfers sowohl innerhalb der Organisation als auch zwischen der Organisation und anderen Parteien bestehen | ☒ | |
| ♦ Verschlüsselung von mobilen Datenträgern (wie DVD, USB-Sticks, Festplatte) nach Stand der Technik | ☒ | |
| ♦ Bei E-Mail, Cloud-Plattformen: Transportverschlüsselung von personenbezogenen Daten nach Stand der Technik bei normalem Risiko | ☒ | |
| ♦ Bei E-Mail, Cloud-Plattformen: Transportverschlüsselung und Inhaltsverschlüsselung von personenbezogenen Daten nach Stand der Technik bei hohem Risiko | ☒ | |
| ♦ Bei Messenger: Transport- und Inhaltsverschlüsselung der Nachrichten und Dateien | ☒ | |
| ♦ Sicherstellung der Integrität von personenbezogenen Daten durch digitale Signaturen zumindest bei hohem Risiko | ☒ | |
| ♦ Bei HTTPS: Einsatz von Client-Zertifikaten zum Nachweis der Authentizität bei geschlossenem Nutzerkreis | ☒ | |

## 17. Entwicklung und Auswahl von Software

Datenschutz und Sicherheit müssen frühzeitig bei der Entwicklung von eigenen Softwaresystemen bzw. bei der Auswahl von Softwareprodukten im eigenen Betrieb berücksichtigt werden.

| | 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 | ☒ | |
| ♦ Es findet eine Trennung von Produktivsystem zu Entwicklungs-/Testsystem statt | ☒ | |
| ♦ Den Zugang zum Source-Code bei der Entwicklung von Software beschränken | ☒ | |
| ♦ Keine personenbezogenen Daten oder Zugangsdaten in der Source-Code-Verwaltung ablegen | ☒ | |
| ♦ System- und Sicherheitstests, wie z. B. Code-Scans | ☒ | |
| ♦ Datensätze sind mit Zweckattributen versehen (z.B. Text- oder Zahlenfeld mit Namen, Größe oder auch Metadaten wie Keyword, Titel oder die H1Überschrift in einer HTML-Definition) | ☒ | |
| ♦ Festlegung von Datenbankrechten entsprechend dem Rollen- Rechtekonzept | ☒ | |

| | | |
|---|---|---|
| ♦ Mandantenfähigkeit relevanter Anwendungen | ☒ | |
| ♦ Physikalische Trennung (Systeme / Datenbanken / Datenträger) | ☒ | |
| ♦ Ausreichende Testzyklen werden berücksichtigt | ☒ | |
| ♦ Fortlaufendes Inventarisieren der Versionen von Software oder Komponenten (z. B. Frameworks, Bibliotheken) sowie deren Abhängigkeiten | ☒ | |
| ♦ Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen | ☒ | |
| ♦ Sicherstellung, dass ein fortlaufender Plan zur Überwachung, Bewertung und Anwendung von Updates oder Konfigurationsänderungen für die gesamte Lebenszeit einer Softwareanwendung besteht | ☒ | |

## 18. Auftragsverarbeiter

Dienstleister, die personenbezogene Daten im Rahmen unserer Auftragsverarbeitung behandeln, benötigen geeignete Garantien, damit auch die Sicherheit der Verarbeitung gewährleistet werden kann.

| | durch | |
|---|---|---|
| | UN | DL |
| ♦ Nur Dienstleister verwenden, die die Garantien (in Form von Dokumenten) zur Verfügung stellen können | ☒ | |
| ♦ 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 | ☒ | |
| ♦ Die Wirksamkeit der Garantien wird durch geeignete Zertifizierungen (ansatzweise) nachgewiesen werden – Bsp.: ISO 27001 bei Rechenzentrum mit Scope Physikalische Sicherheit ist meist aussagekräftig | ☒ | |
| ♦ Eine Vor-Ort-Kontrolle durch den Verantwortlichen wird nicht ausgeschlossen werden | ☒ | |
| ♦ Der Auftragsverarbeiter darf keine weiteren Subdienstleister ohne Information des Auftraggebers aufnehmen – dieser hat dann ein Widerspruchsrecht | ☒ | |
| ♦ Der Auftragsverarbeiter muss Prozesse bei der Erkennung von Datenschutzverletzungen haben und diese unverzüglich dem Verantwortlichen im Sinne der DS-GVO melden | ☒ | |
| ♦ Transfers in unsichere Drittländer sind ggf. nur mit weiteren technischen Schutzmaßnahmen, primär dem Einsatz von kryptographischen Verfahren, möglich | ☒ | |
| ♦ Daten werden bei Auftragsverarbeitung (spätestens) nach Vertragsende wirksam gelöscht | ☒ | |
| ♦ Angaben zur Löschmethodik können bei Bedarf zur Verfügung gestellt werden | ☒ | |
| ♦ Regelmäßige Überprüfung des Auftragsverarbeiters bezüglich Sicherheitspraktiken und Dienstleistungserbringung | ☒ | |
| ♦ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen (z.B. in einem VVT) | ☒ | |

| | | |
|---|---|---|
| ♦ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen (z.B. Postausgangsbuch, Outlook-, Thunderbirdverlauf) | ☒ | |
| ♦ Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen | ☒ | |
| ♦ Persönliche Übergabe papiergebundener Dokumente mit Protokoll (z.B. Abholschein Aktenvernichter, Rückschein bei Einschreiben) | ☒ | |
| ♦ Weitergabe in anonymisierter oder pseudonymisierter Form (z.B. für statistische Zwecke) | ☒ | |
| ♦ Sichere Transportbehälter für papiergebundene Dokumente (z.B. Post-Container, verschließbare Daten-Mülltonnen) | ☒ | |
| ♦ Regelmäßige Überprüfung des Auftragsverarbeiters bezüglich Sicherheitspraktiken und Dienstleistungserbringung | ☒ | |
| ♦ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus | ☒ | |
| ♦ Der Auftragsverarbeiter darf keine weiteren Subdienstleister ohne Information des Auftraggebers aufnehmen – dieser hat dann ein Widerspruchsrecht | ☒ | |
| ♦ Der Auftragsverarbeiter muss Prozesse bei der Erkennung von Datenschutzverletzungen haben und diese unverzüglich dem Verantwortlichen im Sinne der DSGVO melden | ☒ | |
| ♦ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis | ☒ | |
| ♦ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht | ☒ | |

**Ausgefüllt für die Organisation durch**

| | |
|---|---|
| Name | Mark Henkel |
| Funktion | Geschäftsführung und IT Service |
| Rufnummer | 03683-4661872 |
| E-Mail | mark.henkel@dsign-systems[at]de |

Ort, Datum Schmalkalden, 19.11.2021

**Vom Prüfer auszufüllen:**

Geprüft am 20.11.21 durch Karsten Greibel (Date Protection Risk Manager, ICO CISIS12 Porfessional).

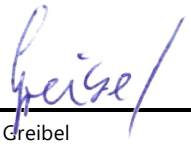
Ergebnis(se):

Nach dem ausführlichen Audit der Geschäftsstelle in Schmalkalden am 20.11.2021 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.

☒ TOM sind für den angestrebten Schutzzweck ausreichend

☒ Vereinbarung Auftragsverarbeitung kann geschlossen werden

Meiningen, 20.11.2021
Ort, Datum

X 

Karsten Greibel
Data Protection Risk Manager (FOM)

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

Die nachfolgenden Ausführungen beziehen sich in spezifizierter Weise auf die Datensicherheits- und Datenschutzeinstellung unserer Servicepartner (siehe Punkt 6.), welche von uns ausführlich geprüft und genutzt werden.

Die aufgeführten Maßnahmen werden zusätzlich zu den allgemeinen technischen und organisatorischen Maßnahmen der Firma dSign Systems GmbH unter Zuhilfenahme ausgewählter Dienstleister (siehe Punkt 6.) umgesetzt.

Die Dokumente allgm_TOM_DSign und spez_TOM_WebApp_Taskcards bilden das vollständige Sicherheitskonzept der Anwendung ab.

## 1. Vertraulichkeit (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.

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

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

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

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.

## 2. Integrität (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

Eingabekontrolle

*Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

Es werden folgende Maßnahmen umgesetzt:

Protokollierung der Eingaben, Dokumentation der Eingabeberechtigungen

## 3. Verfügbarkeit, Belastbarkeit, Desaster 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

## 4. Datenschutzorganisation der Hosting Anbieter/Servicepartner

Unsere eingesetzten Hosting Anbieter/Servicepartner haben aufgrund Ihrer Zertifizierungen ein eigenständiges Datenschutz- und Informationssicherheitsmanagementsystem. Das System umfasst u.a.:

Festlegung von Verantwortlichkeiten, Umsetzung und Kontrolle geeigneter Prozesse, Melde- und Freigabeprozess, Umsetzung von Schulungsmaßnahmen, Verpflichtung der Mitarbeiter und Dienstleister auf Vertraulichkeit, Regelungen zur internen Aufgabenverteilung, Beachtung von Funktionstrennung und -zuordnung, Einführung einer geeigneten Vertreterregelung

## 5. Auftragskontrolle

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.

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 Hosting Anbieter und Servicepartner erfolgt ausschließlich unter Berücksichtigung geeigneter Garantien. Vor Inanspruchnahme der Dienstleistungen wurden die entsprechenden Abschlüsse von Vereinbarung zur Auftragsverarbeitung geschlossen.

Als Hosting Anbieter/Servicepartner 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

## 6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Die ausgewählten Hosting Anbieter/ Servicepartner 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 Hosting Anbieter / der Servicepartner bzw. deren Rechenzentren sind ausschließlich im europäischen Wirtschaftsraum.

| Name / Anschrift | Ort der Verarbeitung | Zertifizierungen | Informationen zur IT-Sicherheit |
|---|---|---|---|
| STRATO AG, Pascalstraße 10, 10587 Berlin | Deutschland | ISO/IEC 27001:2013 | STRATO-Sicherheitskonzept |
| OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken Teil der Unternehmensgruppe OVH SAS-Gruppe | Deutschland, Frankreich / ausschließlich EWR zur Redundanten Speicherung und Sicherstellung der Backup-Strategie | ISO/IEC 27001:2013<br>ISO/IEC 27001<br>SOC 1, 2, 3<br>ANSSI SecNumCloud<br>PCI DSS Level 1<br>C5 Katalog BSI | OVHcloud Sicherheitspolitik |
| billwerk GmbH Mainzer Landstraße 51, 60329 Frankfurt am Main | Deutschland, Frankreich / EWR | AWS-Rechenzentren EU: ISO/IEC 27001:2013 | |