

Anlage 2 zur AVV
Technische und organisatorische Maßnahmen

Ziel: Dokumentation der Technischen und organisatorischen Maßnahmen in der ics cloud services GmbH.

Version	Stand	Bemerkung
1.0	05.04.24	Aktualisierung TOM nach Abschluss einer IST-Analyse durch den DSB.
1.2	04.12.25	Aktualisierung nach Abschluss der ISO/IEC 27001 Zertifizierung.

Referenz DS-GVO	Referenz ISO/IEC 27001	Thema	Beschreibung	technische Maßnahmen	organisatorische Maßnahmen	Bemerkung
Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)	A.7.1, A.7.2, A.7.3, A.7.4, A.7.6	Zutrittskontrolle	Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z. B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen. Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chip-karten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.	<ul style="list-style-type: none"> - Alarmanlage - Manuelles Schließsystem - Sicherheitsschlösser - Klingelanlage mit Kamera - Türsicherung (elektronischer Türöffner) 	<ul style="list-style-type: none"> - Schlüsselregelung - Besucher in Begleitung durch Mitarbeiter - Sorgfalt bei Auswahl Reinigungsdienste - Dokumentation zur physischen Sicherheit 	
Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)	A.5.15, A.5.16, A.5.17, A.8.1, A.8.3, A.8.5, A.6.7, A.7.7	Zugangskontrolle	Keine unbefugte Systembenutzung, z. B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern. Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).	<ul style="list-style-type: none"> - Login mit Benutzername + Passwort - Login mit biometrischen Daten - Anti-Viren-Software Server - Anti-Virus-Software Clients - Firewall - Mobile Device Management - Einsatz VPN bei Remote-Zugriffen - Verschlüsselung von Datenträgern - Verschlüsselung Smartphones - Automatische Desktopsperrung - Verschlüsselung von Notebooks/Tablets - Protokollierung der Anmeldeversuche und Abbruch des Anmeldevorgangs nach festgelegter Zahl von erfolglosen Versuchen 	<ul style="list-style-type: none"> - Verwalten von Benutzerberechtigungen - Erstellen von Benutzerprofilen - Zentrale Passwortvergabe - Richtlinie Authentifizierungsmaßnahmen - Richtlinie Identitäts- und Zugriffsmanagement - Richtlinie Clear Desk und Screen - Richtlinie Datenschutz/Sicherheit - Richtlinie verteiltes Arbeiten 	

<p>Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) A.5.18, A.8.2</p>	<p>Zugriffskontrolle</p>	<p>Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen. Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.</p>	<ul style="list-style-type: none"> - Aktenshredder - Physische Löschung von Datenträgern - Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten 	<ul style="list-style-type: none"> - Einsatz Berechtigungskonzepte - Minimale Anzahl an Administratoren - Verwaltung Benutzerrechte - Richtlinie Identitäts- und Zugriffsmanagement
<p>Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) A.8.22, A.8.31, A.5.3</p>	<p>Trennungskontrolle</p>	<p>Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit, Sandboxing. Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.</p>	<ul style="list-style-type: none"> - Trennung von Produktiv- und Testumgebung - Mandantenfähigkeit relevanter Anwendungen 	<ul style="list-style-type: none"> - Steuerung über Berechtigungskonzept - Festlegung von Datenbankrechten - ISMS-Leitlinie - Netzwerktrennung
<p>Pseudonymisierung (Art. 32 Abs. 1 lit. a) DS-GVO; Art. 25 Abs. 1 DS-GVO) A.8.11, A.8.24, A.8.12</p>	<p>Pseudonymisierung</p>	<p>Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.</p>	<ul style="list-style-type: none"> - Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten System (mögl. verschlüsselt) - Hashwertverfahren (SHA-2; SHA-3) 	<ul style="list-style-type: none"> - Richtlinie Datenverfügbarkeit und Informationsschutz - Kryptographiekonzept - Verfahren zur Datenmaskierung

<p>Integrität (Art. 32 Abs. 1 lit. b DS-GVO) A.5.14, A.8.20, A.7.10, A.7.14</p>	<p>Weitergabekontrolle</p>	<p>Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur Maßnahmen, die 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.</p> <ul style="list-style-type: none"> - E-Mail-Verschlüsselung - Einsatz von VPN - Protokollierung der Zugriffe und Abrufe - Bereitstellung über verschlüsselte Verbindungen wie sftp, https - Verschlüsselungsverfahren, die Datenveränderungen während des Transports aufdecken - Sicherer Transportbehälter für Datenträger <ul style="list-style-type: none"> - Weitergabe in anonymisierter oder pseudonymisierter Form - Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen - Transportprozesse mit individueller Verantwortlichkeit - Asset Management - Verfahren zur Informationsklassifizierung
<p>Integrität (Art. 32 Abs. 1 lit. b DS-GVO) A.8.10, A.8.15, A.8.16, A.8.17</p>	<p>Eingabekontrolle</p>	<p>Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung, Dokumentenmanagement. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.</p> <ul style="list-style-type: none"> - Technische Protokollierung der Eingabe, Änderung und Löschung von Daten - Manuelle oder automatisierte Kontrolle der Protokolle <ul style="list-style-type: none"> - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts - Richtlinie Ereignisprotokollierung - Uhrensynchronisation

<p>Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)</p> <p>A.8.7, A.7.11, A.7.5, A.8.14, A.5.19, A.8.8, A.8.6, A.8.19</p>	<p>Verfügbarkeitskontrolle</p>	<p>Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.</p> <p>Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.</p>	<ul style="list-style-type: none"> - Virenschutz - Firewall - regelmäßige Erstellung von Backups - Überwachung der Systemzustände 	<ul style="list-style-type: none"> - Backup & Recovery-Konzept - Kontrolle des Sicherungsvorgangs - Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse - Keine sanitären Anschlüsse im oder oberhalb des Serverraums - Existenz eines Notfallplans - Getrennte Partitionen* für Betriebssysteme und Daten - Redundanz der informationsverarbeitenden Einrichtungen - Verfahren zum Management von Lieferantenbeziehungen 	<p>Systeme sind in ausgelagerten deutschen Rechenzentren gehostet, diese erfüllen die erforderlichen technischen und organisatorischen Maßnahmen an einen sicheren Betrieb. Für weitere Informationen siehe Liste der Unterauftragnehmer (Linkeinfügen.de)</p>
<p>Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c) DS-GVO)</p> <p>A.8.13, A.5.29, A.5.30</p>	<p>Rasche Wiederherstellung</p>	<p>Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne</p>	<ul style="list-style-type: none"> - Virenschutz - Firewall - regelmäßige Erstellung von Backups - Überwachung der Systemzustände 	<ul style="list-style-type: none"> - Backupkonzept mit Datenvorhaltung vor Ort und redundant an einem weiteren Standort - Notfallhandbuch 	<p>Systeme sind in ausgelagerten deutschen Rechenzentren gehostet, diese erfüllen die erforderlichen technischen und organisatorischen Maßnahmen an einen sicheren Betrieb. Für weitere Informationen siehe Liste der Unterauftragnehmer (Linkeinfügen.de)</p>
<p>Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)</p> <p>A.5.1, A.5.35, A.6.3, A.5.4, A.5.34, A.5.2, A.5.36, A.6.2, A.5.37</p>	<p>Datenschutz-Management</p>	<p>Prozess zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Dies dient der Sicherstellung, dass die Sicherheit der Verarbeitung kontinuierlich gewährleistet ist und an neue Risiken oder technische Entwicklungen angepasst wird (Kontinuierlicher Verbesserungsprozess).</p>	<ul style="list-style-type: none"> - Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z. B. Wiki, Intranet ...) - Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt 	<ul style="list-style-type: none"> - externer Datenschutzbeauftragter - Zertifizierung nach ISO/IEC 27001 - Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet - Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich - Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt - Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach - Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden 	

<p>Sicherheit personenbezogener Daten (Art. 33 DS- GVO, Art. 34 DS- GVO)</p> <p>A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.8</p>	<p>Incident-Response-Management</p>	<p>Maßnahmen zur unverzüglichen Erkennung, Eindämmung und Meldung von Verletzungen des Schutzes personenbezogener Daten. Ziel ist es, Sicherheitsvorfälle schnellstmöglich zu beheben und das Risiko für die Rechte und Freiheiten natürlicher Personen zu minimieren sowie gesetzliche Meldepflichten (72h) einzuhalten.</p>	<ul style="list-style-type: none"> - Einsatz von Firewall und regelmäßige Aktualisierung - Einsatz von Spamfilter und regelmäßige Aktualisierung - Einsatz von Virens Scanner und regelmäßige Aktualisierung 	<ul style="list-style-type: none"> - Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde - Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen - Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen - Dokumentation von Sicherheitsvorfällen und Datenpannen z. B. via Ticketsystem - Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
<p>Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS- GVO)</p> <p>A.8.25, A.8.9, A.8.32</p>	<p>Datenschutzfreundliche Voreinstellung</p>	<p>Umsetzung technischer und organisatorischer Maßnahmen, die sicherstellen, dass standardmäßig nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.</p>	<ul style="list-style-type: none"> - Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen 	<ul style="list-style-type: none"> - Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

<p>Auftragsverarbeiter (Art. 28 DS-GVO) A.5.19, A.5.20, A.5.21, A.5.22, A.5.23</p>	Auftragskontrolle	<p>Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen. Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.</p>	<ul style="list-style-type: none"> - Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit) - Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard Vertragsklauseln - Schriftliche Weisungen an den Auftragnehmer - Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis - Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellopflicht - Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer - Regelung zum Einsatz weiterer Subunternehmer - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags - Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
--	--------------------------	---	---