Auftragsverarbeitungsvertrag (AVV) zur Erbringung von Support-, Pflege- und Dienstleistungen

zwischen dem

Auftraggeber

und der

Procilon GmbH,
gesetzlich vertreten durch die Geschäftsführung,
Nikolaistraße 12/14, 04109 Leipzig

- nachstehend Auftragnehmer genannt -

Präambel

(1) Die Procilon GmbH und die Procilon Group Services GmbH erbringen Leistungen im Bereich IT-Sicherheit, die im Hauptvertrag näher spezifiziert sind.

(2) Der Auftragnehmer dieser Vereinbarung entspricht dem Auftragnehmer des Hauptvertrages. Darüber hinaus erbringen die Mitglieder innerhalb der Unternehmensgruppe Leistungen, weshalb sie als Subunternehmer auftreten können. Die Mitglieder der Procilon Unternehmensgruppe verfügen über ein einheitliches Datenschutz- und Informationssicherheitsniveau.

(3) Die EU-Datenschutz Grundverordnung (DSGVO) verpflichtet Verarbeiter von personenbezogenen Daten in Art. 28 Abs. 3 eine Vereinbarung zur Auftragsdatenverarbeitung zu schließen. Im Rahmen dieses Auftragsverarbeitungsvertrages verpflichtet sich die Procilon GmbH gegenüber dem Auftraggeber.

1 Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) ggf. auch in Verbindung mit § 80 Sozialgesetzbuch Zehntes Buch – SGB X und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der „Verarbeitung" in Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2 Gegenstand der Vereinbarung

(1) Gegenstand der Vereinbarung sind zu erbringende Support- und Softwarepflegeleistungen sowie Dienstleistungen zu Produkten entsprechend dem Hauptvertrag.

(2) Folgende Datenarten können auftreten und verarbeitet werden:

- Kontaktdaten (z.B. Name, Anschrift, E-Mail, Telefon, Beruf, Titel)
- Technische Daten der Kommunikation (z.B. Message ID, Log-Daten, Zugangsdaten, OSCI-Kennungen)
- Identitätsdaten (z.B. Ausweiskopien, Beglaubigungsvermerke, Kopien von sonstigen Urkunden, Bank- und Finanzdaten)
- Besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO (z.B. Gesundheitsdaten, Sozialdaten, Steuerdaten)
- Support- und Lizenzberechtigung

(3) Betroffene Personen können sein:

- Mitarbeiter des Auftraggebers
- Mitarbeiter von Endkunden des Auftraggebers
- Mitarbeiter des Auftragnehmers
- Patienten, Klienten

3 Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen dieser AVV getroffenen Vereinbarungen. Der Auftraggeber kann zusätzliche Weisungen erteilen, soweit dies zur Einhaltung des anwendbaren Datenschutzrechts erforderlich ist.

(2) Der Auftragnehmer verpflichtet sich zur Entgegennahme von Weisungen Ansprechpartner zur Verfügung zu stellen.

(3) Der Auftragnehmer verpflichtet sich zur Entgegennahme von Weisungen. Sie können gerichtet werden an den jeweiligen vertrieblichen Ansprechpartner oder an den Datenschutzbeauftragten des Auftragnehmers

Datenschutz@procilon.com

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine erteilte Weisung nach seiner Meinung gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Verantwortlichen des Auftraggebers bestätigt oder geändert wird.

(5) Der Auftragnehmer setzt technische und organisatorische Maßnahmen (TOMs) zum Schutz der Daten des Auftraggebers um. Diese sind in Anlage 2 aufgeführt.

(6) Der Auftragnehmer überprüft regelmäßig die auftrags- und datenschutzkonforme Durchführung des Vertrages.

(7) Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO werden im Rahmen der Supportbearbeitung nicht gespeichert. Nach Abschluss eines Supportfalls werden die personenbezogenen Daten in der Supportanwendung gelöscht. Soweit Informationen aus dem Supportfall für die technische Weiterentwicklung der Software erforderlich sind, erfolgt eine Anonymisierung der Daten vor weiterer Verarbeitung. Die Anonymisierung erfolgt so, dass ein Personenbezug gemäß Art. 4 Nr. 1 DSGVO ausgeschlossen ist.

(8) Der Auftragnehmer ist verpflichtet den Auftraggeber unverzüglich zu informieren, falls ein Verstoß gegen datenschutzrechtliche Vorschriften oder gegen diese AVV oder Weisungen des Auftraggebers erfolgt ist, durch Mitarbeiter des Auftragnehmers oder andere mit der Verarbeitung betrauten Personen.

(9) Ebenso wird der Auftragnehmer den Auftraggeber unverzüglich informieren, falls eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies eine Kontrolle der Datenverarbeitung der Auftraggeberdaten betreffen kann.

(10) Sollte der Auftragnehmer feststellen, dass ihm vom Auftraggeber personengebundene Daten unrechtmäßig übermittelt wurden, so informiert der Auftragnehmer den Auftraggeber unverzüglich nach Art. 33 Abs 3 DSGVO.

(11) Der Auftragnehmer ist verpflichtet, Beschwerden und Eingaben im Zusammenhang mit diesem Vertrag unverzüglich an den Auftraggeber weiterzuleiten.

(12) Der Auftragnehmer unterstützt den Auftraggeber bei der Erstellung eines Verarbeitungsverzeichnisses und wird notwendige Informationen zur Verfügung stellen.

(13) Der Auftragnehmer verpflichtet sich, den Auftraggeber im Rahmen seiner Möglichkeiten und nach Weisung bei der Bearbeitung von Anfragen und der Geltendmachung von Rechten betroffener Personen gemäß Art. 12 bis 22 DSGVO zu unterstützen. Dies umfasst insbesondere das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung,

Datenübertragbarkeit sowie Widerspruch. Die Unterstützung erfolgt unverzüglich und unter Berücksichtigung der gesetzlichen Fristen.

(14) Der Auftragnehmer verpflichtet sich darüber hinaus, den Auftraggeber bei der Einhaltung der Pflichten gemäß Art. 32 bis 36 DSGVO zu unterstützen. Dies umfasst insbesondere die Umsetzung und Dokumentation technischer und organisatorischer Maßnahmen zur Datensicherheit, die Mitwirkung bei der Meldung von Datenschutzverletzungen gemäß Art. 33 und 34 DSGVO sowie die Unterstützung bei der Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO und der Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO. Der Auftragnehmer unterstützt den Auftraggeber - soweit - vereinbart im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Art. 28 Abs. 3 lit. f) DSGVO.

4 Benennung eines Datenschutzbeauftragten

Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Für Procilon GmbH ist Frau Ulrike Zenker, erreichbar unter der E-Mailadresse Datenschutz@procilon.com, Nikolaistraße 12/14, 04109 Leipzig. Ein Wechsel der Beauftragten wird unter www.procilon.com/Datenschutz angezeigt.

5 Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 5.1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die von dem Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 5.1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dafür Sorge tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sodass Betriebsabläufe nicht gestört werden.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber nach Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen durch den Auftragnehmer zu informieren.

6 Unterauftragnehmer

(1) Als Unterauftragnehmer im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

(2) Der Aufragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der personenbezogenen Daten des Auftraggebers auf bei ausgelagerten

Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(3) Der Auftragnehmer nimmt die Dienste von Unterauftragnehmern in Anspruch. Der Auftraggeber stimmt der Beauftragung der in Anlage 1 aufgeführten Subunternehmen mit Abschluss dieser AVV zu. Für die Hinzuziehung weiterer oder die Ersetzung einzelner oder aller in Anlage 1 genannten Subunternehmer gilt Satz 1 entsprechend. Der Auftragnehmer informiert den Auftraggeber rechtzeitig über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragnehmers und ermöglicht einen Widerspruch.

(4) Der Auftragnehmer hat die Subunternehmen sorgfältig auszuwählen und vor Beauftragung zu prüfen, dass die zwischen dem Auftraggeber und dem Auftragnehmer getroffenen Vereinbarungen eingehalten werden können. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass die Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen haben.

(5) Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. § 38 BDSG bzw. Art. 37 DSGVO bestellt hat.

(6) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber den Subunternehmern gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(7) Der Auftragnehmer schließt mit den Subunternehmern jeweils einen Auftragsverarbeitungsvertrag. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(8) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 5 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte des Auftraggebers und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

7 Datengeheimnis

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des § 53 BDSG bzw. nach Art. 28 Abs. 3 Buchst. b) DSGVO zu Wahrung der Vertraulichkeit verpflichtet. Diese Verpflichtung besteht auch nach Beendigung des Vertrages fort.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. § 53 BDSG bzw. nach Art. 28 Abs. 3 Buchst. b) DSGVO verpflichtet werden. Soweit Sozialdaten i.S.d. § 67 Abs. 2 SGB X verarbeitet werden, sind die Mitarbeiter des Auftragnehmers auch auf das Sozialgeheimnis zu verpflichten.

(3) Diese Verpflichtung der beschäftigten Mitarbeiter ist auf Anfrage dem Auftraggeber nachzuweisen.

8 Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

9 Dauer des Auftrags

(1) Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Rahmenvertrages/Hauptvertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben. Dieser Vertrag kann nicht getrennt vom Hauptvertrag gekündigt werden.

(2) Das Recht zum Ausspruch einer außerordentlichen Kündigung durch die Parteien wird durch vorstehende Bestimmungen nicht eingeschränkt. Der Auftraggeber kann den Vertrag insbesondere jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert. Der Auftragnehmer kann den Vertrag insbesondere jederzeit kündigen, wenn ein schwerwiegender Verstoß des Auftraggebers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftraggeber die vertraglich vereinbarte Vergütung trotz erfolgloser Nachfristsetzung nicht zahlt oder an offensichtlich rechtswidrigen Weisungen zur Datenverarbeitung trotz entsprechendem Hinweis des Auftragnehmers festhält.

10 Haftung

Für Schadenersatzansprüche, die Betroffene gegenüber dem Auftragnehmer wegen eines Verstoßes aus diesem Vertrag geltend machen, gilt die gesetzliche Regelung. Gegenüber betroffenen Personen haften Auftraggeber und der Auftragnehmer gemäß der in Art. 82 DSGVO getroffenen Bestimmung.

11 Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungsergebnisse, die im Zusammenhang mit dem Vertragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer, die jedoch den Löschfristen des Auftragnehmers für Backups unterliegen. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Löschung der Daten bei dem Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

12 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers bei dem Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.
Für Nebenabreden zu diesem Vertrag ist die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

(3) Als Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag stehenden Streitigkeiten wird Leipzig vereinbart.

Anlage 1: Liste der Subunternehmer

Dienstleister	Dienstleistung	Ort der Datenverarbeitung
Microsoft Ireland Operations Limited 70 Sir John Rogerson's Quay Dublin 2, D02 R296 Irland	Hosting Azure Cloud Germany für SaaS Leistungen Microsoftanwendungen (Office) Nextcloud (Archiver)	Europa
Hetzner Online GmbH, Gunzenhausen Industriestr. 25 91710 Gunzenhausen	Hosting Interne Tests, eBo, nextcloud (Archiver), CRM	Deutschland
Procilon Group Services GmbH Nikolaistraße 12/14 04109 Leipzig / Schützenstraße 52 10117 Berlin	Accounting, Legal, Corporate Services	Deutschland
DARZ GmbH Julius-Reiber Straße 11 64293 Darmstadt	Hosting Nextcloud (Archiver), CRM (ab Q4 2025)	Deutschland
Capita Customer Services (Germany) GmbH Rudower Chaussee 4 12489 Berlin	Call Center	Deutschland
TeamViewer Germany GmbH Jahnstraße 30 73037 Göppingen	Remote log in	Deutschland

(4) Anlage 2: Technische und organisatorische Maßnahmen (TOMs)

i. S. d. Art. 32 DSGVO des Auftragnehmers

Technische und Organisatorische Maßnahmen der Procilon GmbH

Gem. Artikel 32 DSGVO

Inhalt

Präambel 3
1 Vertraulichkeit (Art. 32 Abs. 1 lit b DSGVO) 4
1.1 Zutrittskontrollen 4
1.2 Zugangskontrollen 5
1.3 Zugriffskontrolle 6
1.4 Trennungskontrolle 6
2 Integrität (Art. 32 Abs. 1 lit. B DSGVO) 7
2.1 Weitergabekontrolle 7
2.2 Eingabekontrolle 7
3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit b DSGVO) 8
3.1 Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit 8
3.2 Sicherungskonzept 8
4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO) 9
4.1 Datenschutzmanagement 9
4.2 Informationssicherheitsmanagement 9
4.3 Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung 10
4.4 Auftragskontrolle 10
5 Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten bei mobiler Arbeit gemäß Art. 32 DSGVO 10
6 Sonstiges 11
7 Änderungshistorie 11

Präambel

(1) Die Procilon Group Services GmbH stellt für die Procilon GmbH zentrale Funktionen, unter anderem den Bereich Legal zur Verfügung. Sie hat die Aufgabe Regelungen zu Datenschutz und Informationssicherheit im Rahmen der Gruppe zu vereinheitlichen und ein entsprechendes Datenschutz- und Informationssicherheitsmanagement aufzusetzen.

(2) Die EU-Datenschutz Grundverordnung (DSGVO) verpflichtet Verarbeiter von personenbezogenen Daten in Art. 32 dazu geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(3) Die folgenden Kapitel beschreiben die von Procilon GROUP getroffenen Maßnahmen in Bezug auf den Schutz von personengebunden Daten. Diese Maßnahmen gelten für die Procilon GROUP GmbH mit ihren Töchtern Procilon GmbH und intarsys GmbH, diese mit ihrer Tochter intarsys (Schweiz) AG.

(4) Die Lokationen der Procilon sind:

Sitz der Procilon Group Services GmbH und der Procilon GmbH	Nikolaistraße 12-14 04109 Leipzig
weitere Niederlassungen der Procilon Group Services GmbH und der Procilon GmbH	Schützenstraße 8 10117 Berlin
weitere Niederlassungen der Procilon GmbH	Kriegsstraße 236 76135 Karlsruhe

(5) Folgende technische und organisatorische Maßnahmen werden von der Procilon zur Sicherung personengebundener Daten umgesetzt:

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

1.1 Zutrittskontrollen

(1) Sicherstellung der Zutrittsbeschränkungen zu Datenverarbeitungsanlagen. Dabei wird auf physische Orte der Procilon Unternehmensgruppe eingegangen, sowie auf physische Betriebsorte von SAAS-Anwendungen und RZ-Dienstleistern.

(2) Folgende Zutrittskontrollen sind an den jeweiligen Hauptsitzen realisiert:

	Technische Maßnahmen
x	Alarmanlage
x	Chipkarten-/Transponder-Schließsystem
x	Bewegungsmelder
x	Manuelles Schließsystem
x	Elektronische Sicherheitsschlösser

	Organisatorische Maßnahmen
x	Personenkontrolle beim Pförtner / Empfang
x	Protokollierung der Besucher / Besucherbuch
x	Schlüsselregelung / Schlüsselbuch
x	Sorgfältige Auswahl von Sicherheitspersonal, bei intarsys über Vermieter
x	Sorgfältige Auswahl von Reinigungspersonal
x	Tragepflicht von Gästeausweisen oder Begleitpflicht des Besuchs
x	Sicherheitszonen mit verschiedenen Zutrittsberechtigungen
x	Wachschutz, bei intarsys über Vermieter

(3) Procilon nutzt für ihre cloudbasierten Produkte ausschließlich ISO 27001 zertifizierte Rechenzentren, die ihre Betriebsstätten über eigene technische und organisatorische Maßnahmen absichern. Betriebsort der Rechenzentren ist Deutschland oder Europa, dies ist in der jeweiligen Leistungsbeschreibung des Produktes ausgewiesen.

(4) Zur internen Datenverarbeitung nutzt Procilon eigene Rechenleistung in den abgesicherten IT-Räumen der Lokationen sowie SAAS-Anwendungen, deren Betriebsort ebenfalls in Deutschland oder Europa liegt und damit den Anforderungen der DSGVO unterliegt. Neben den SAAS-Anwendungen werden auch ISO 27001-zertifizierte RZ-Dienstleister als Privat-/Public-Cloud-Anbieter mit Betriebsort Deutschland eingesetzt, die (eigenadministriert) zur Datenverarbeitung genutzt werden.

1.2 Zugangskontrollen

Keine unbefugte Systembenutzung wird durch folgende Maßnahmen erreicht:

	Technische Maßnahmen
x	Authentifikation mit Benutzer + Passwort
x	Zwei-Faktor-Authentifizierung
x	Einsatz von Firewalls
x	Einsatz von Mobile Device Management (Handys)
x	Einsatz von VPN-Technologie
x	Einsatz von Anti-Viren-Software
	Einsatz automatischer Bildschirmschoner

	Organisatorische Maßnahmen
x	Benutzerberechtigungen verwalten
x	Erstellen von Benutzerprofilen
x	Definierte Passwortregeln
x	Passwortrücksetzungsverfahren
x	Regelmäßige Überprüfung der Berechtigungen

Cloud Produkte

Zugang zu Cloud-Produkten für Kunden der **protectr-Plattform** (Dateiverschlüsselung, elektronische Bürger- und Organisationenpostfach (eBO), elektronische Signatur und Siegelung), der Procilon **AS4 Cloud Service**, und der **proGOV-Cloud Service** ist über oben gekennzeichnete Maßnahmen geschützt.

Zugang zu Kundensystemen

Support und Professional Service können Zugang zu Kundensystemen erhalten.:

Direkter remote Zugriff auf Kunden-/Partnersysteme für registrierte VIP-Betreuung im Bereich Professional Service. Diese Zugänge werden vom Auftraggeber kontrolliert und gesichert.

Im Falle von temporären remote Zugriffen im Rahmen Support/Pflege erfolgt der Zugriff über Fernwartungslösungen wie TeamViewer, ergänzend MS Teams. Der Zugang erfolgt durch ausgewiesenes Personal im Bereich Support unter Anwesenheit des Kunden.

Der Zugang zu Kundensystemen wird immer durch den Auftraggeber gewährt und kontrolliert. Eine selbständige Aufschaltung auf die Systeme des Auftraggebers ist dem Auftragnehmer ohne Zutun des Auftraggebers nicht möglich.

Sollte es erforderlich sein, Daten oder Dokumente vom Kundensystem auf die Systeme der Procilon Group zur weiteren Fehleranalyse zu übertragen, werden Auftraggeber und Auftragnehmer einen sicheren Übertragungsweg zur Datenübertragung wählen.

1.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

	technische Maßnahmen
x	Physische Löschung von Datenträgern vor deren Wiederverwendung
x	Protokollierung der Vernichtung von Daten
x	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
x	Verschlüsselung von Datenträgern
x	Vergabe von Berechtigungen nach dem Need-to-know-Prinzip

	organisatorische Maßnahmen
x	Anzahl der Administratoren auf das „Notwendigste" reduzieren
x	Einsatz von Dienstleistern zur Akten- und Datenvernichtung
x	Erstellen eines Berechtigungskonzepts
x	Passwortrichtlinie inkl. Länge und Wechsel
x	Sichere Aufbewahrung von Datenträgern
x	Verwaltung der Benutzerrechte durch Systemadministratoren
x	Mehraugen-Prinzip

1.4 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden durch folgende Maßnahmen umgesetzt:

	technische Maßnahmen
	Anonymisierung von Datensätzen
x	Physisch oder logisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
x	Trennung von Entwicklungs-, Produktiv- und Testsystem

	organisatorische Maßnahmen
x	Erstellung eines Berechtigungskonzepts zwecks Mandantentrennung
x	Festlegung von Datenbankrechten
x	Logische Mandantentrennung (softwareseitig)

2 Integrität (Art. 32 Abs. 1 lit. B DSGVO)

2.1 Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport wird gesichert durch folgende Maßnahmen:

	technische Maßnahmen
x	Einrichtung von VPN-Tunneln
x	E-Mail-Verschlüsselung
x	Verschlüsselung von Anhängen
x	Elektronische Signatur

	organisatorische Maßnahmen
x	Dokumentation der Empfänger von Daten und der Zeitspannen der vereinbarter Löschfristen

2.2 Eingabekontrolle

Die Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement, erfolgt durch folgende Maßnahmen:

	technische Maßnahmen
x	Protokollierung der Eingabe, Änderung und Löschung von Daten

	organisatorische Maßnahmen
	Verwaltung einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
x	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
x	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit b DSGVO)

3.1 Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust und Vorkehrungen, um möglichst schnell die Daten wieder herzustellen, wird durch folgende Maßnahmen erreicht:

	technische Maßnahmen
x	Feuerlöschgeräte in Serverräumen
x	Feuer- und Rauchmeldeanlagen
x	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
x	Klimaanlage in Serverräumen im Hosting-Bereich
x	Schutzsteckdosenleisten in Serverräumen im Hosting-Bereich
x	Unterbrechungsfreie Stromversorgung (USV)
x	Doppelte IT-Infrastruktur (Redundanz) im Hosting-Bereich
x	Regelmäßige Belastungstests im Hosting Bereich

	organisatorische Maßnahmen
x	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen im Hosting Bereich
x	Aufbewahrung von Datensicherung an einem sicheren oder ausgelagerten Ort
x	Erstellen eines Backup- & Recoverykonzepts
x	Erstellen eines Notfallplans (Incident-Responce-Plan)
x	Festlegung von Meldewegen
	Regelmäßige Durchführung von Krisen/-Notfallübungen
x	Testen von Datenwiederherstellung
x	Serverräume nicht unter sanitären Anlagen

3.2 Sicherungskonzept

Unser Sicherungskonzept, sieht folgende Maßnahmen vor:

- Rollierende tägliche Sicherung der Serverlaufwerke und Aufbewahrung der Sicherungsbänder außerhalb des Rechenzentrums.
- Durch Raid-Plattensysteme / automatische Restauration für bis zu 2 Plattenausfälle nach Austausch defekter Teile
- Bei Nutzung von Cloudsystemen werden zentrale Backup-Server genutzt und unanfällige Raid1-Festplattensysteme:

- Täglich automatisches, rollierendes Voll-Backup, bis zu 7 Slots je Server, beim nächsten Backup wird das älteste Backup gelöscht. Manuelle Sicherung (Snapshot) möglich.

- Sicherheitsupdates werden kontinuierlich eingepflegt.
- Die Überwachung der IT-Systeme erfolgt durch Monitoring.
- Die Überwachung externer RZ-Betriebsstätten obliegt den RZ-Betreibern/Hostern. Ein Monitoring der Lösungen erfolgt innerhalb der Procilon GROUP.

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

4.1 Datenschutzmanagement

	organisatorische Maßnahmen
x	Bestellung eines Datenschutzbeauftragten
x	Regelmäßiges Berichtswesen an die Geschäftsführung
x	Datenschutzkonzept
x	Eskalationsverfahren für Notfälle
	Regelmäßige Auditierung / Zertifizierung durch Externe
x	Regelmäßige interne Überprüfung / Aktualisierung der getroffenen Maßnahmen gemäß dem Stand der Technik (durch DSB, IT-Revision etc.)

4.2 Informationssicherheitsmanagement

	technische Maßnahmen
x	Regelmäßige Penetrationstests
x	Regelmäßige Prüfung der Hardware (Lifecycle, Performance)
x	Incident-Response-Management (I-R-Planung)

	organisatorische Maßnahmen
x	IT-/Informationssicherheitsbeauftragter
x	Regelmäßiges Berichtswesen an die Geschäftsführung
x	Informations-/IT-Sicherheitskonzept
x	Eskalationsverfahren für Notfälle
x	Regelmäßige interne Überprüfung / Aktualisierung der getroffenen Maßnahmen gemäß der anerkannten Regeln der Technik (durch DSB, ISB, etc.)

Erarbeitung eines ISMS-Systemsaufbaus zur Erlangung einer ISO-Zertifizierung 27001.

4.3 Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung

	technische Maßnahmen
x	Verwendung von Opt-In-Lösungen
x	Minimierung von Pflichtfeldern
x	Deutliche Kennzeichnung von freiwilligen Angaben
x	Beschränkung der Angaben und weiteren Verwendung auf das notwendige Maß

	organisatorische Maßnahmen
x	Regelungen zur Datenminimierung, Datensparsamkeit und Erforderlichkeit
x	Einhaltung von Branchenstandards

4.4 Auftragskontrolle

	technische Maßnahmen
x	Überprüfung aller vertraglich zugesicherten technischen Maßnahmen (ggf. vor Ort)

	organisatorische Maßnahmen
x	Auswahl von Auftragsverarbeitern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
x	Vorherige Prüfung der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen und entsprechende Dokumentation mit Nachweisen
x	Regelmäßige Überprüfung der Auftragsverarbeiter hinsichtlich Datenschutzes / Datensicherheit
x	Abschluss von Verträgen zur Auftragsverarbeitung unter Berücksichtigung aller gesetzlichen Anforderungen gemäß Art. 28 DS-GVO

5 Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten bei mobiler Arbeit gemäß Art. 32 DSGVO.

	technische Maßnahmen
x	Verschlüsselung mobiler Endgeräte (z. B. BitLocker, FileVault) zur Sicherung bei Verlust oder Diebstahl
x	VPN-Zugang mit zertifikatsbasierter Authentifizierung für Zugriff auf interne Ressourcen.
x	Entra ID von Microsoft zur Authentifizierung über Single Sign On für Mitarbeiter zum Zugriff über webbasierte Clouddienste.
x	Zwei-Faktor-Authentifizierung für alle externen Zugriffe

x	Mobile Device Management (MDM) zur zentralen Verwaltung und Absicherung mobiler Geräte
x	Sichtschutzfolien für Bildschirme bei Nutzung in öffentlichen Bereichen
x	Automatische Sperrung der Geräte bei Inaktivität
x	Firewall und Antivirus-Software auf allen mobilen Geräten

	organisatorische Maßnahmen
x	Schulung der Mitarbeitenden zu Risiken und Schutzmaßnahmen beim mobilen Arbeiten.
x	Clean Desk & Clear Screen Policy auch im häuslichen Umfeld.
x	Verbot der Nutzung vertraulicher Daten in öffentlichen Räumen (z. B. ÖPNV, Cafés, Hotels).
x	Verpflichtung zur sicheren Aufbewahrung der Geräte außerhalb der Arbeitszeit (z. B. verschlossener Schrank).
x	(Heim-)Netzwerksicherheit durch WPA2/WPA3 und komplexe Passwörter
x	Meldungspflicht bei Verlust oder Diebstahl von Geräten oder Daten.

6 Sonstiges

Dieses Dokument wird rollierend überprüft und an situativen Änderungen angepasst.

7 Änderungshistorie

Version	Bearbeiter	Bemerkung	Fertigstellung
01-1	Hmü / uz	Entwurf TOM Procilon GROUP: Zusammenführung der TOM der Procilon GmbH und intarsys GmbH	16.06.2025
01-2	uz	Trennung und Präzisierung der Unterstützungs-pflichten des Auftragnehmers gemäß Art. 28 Abs. 3 Aufnahme von Finanzdaten in den Arten von personenbezogenen Daten	16.07.2025
02	Hmü / uz	Aufnahme von Maßnahmen zum mobilen Arbeiten	03.09.2025
03	uz	Ergänzung Entra-ID unter „5 Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit personen-bezogener Daten bei mobiler Arbeit gemäß Art. 32 DSGVO“	16.11.2025
04	uz	Abbildung der Verschmelzung der Intarsys GmbH auf die Procilon GmbH, Berücksichtigung der Procilon Group Service GmbH als neue Zentralfunktion	04.09.2026

In diesem Dokument wird zur Vereinfachung das generische Maskulin verwendet.
Das generische Maskulin steht stellvertretend für alle Geschlechter.