Vereinbarung über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

PROVENTOR - Software as a Service

abgeschlossen zwischen

Auftragsverarbeiter:

PROVENTOR e-solutions GmbH
Kärntner Straße 337
A-8054 Graz, Austria

sowie alle zugehörigen Tochterunternehmen

Verantwortlicher bzw. Auftraggeber:

Kunden sowie Interessenten von PROVENTOR e-solutions GmbH sowie zugehörigen Tochterunternehmen welche ein PROVENTOR System für den produktiven Einsatz oder zu Test und Demozwecke nutzen.

März 2026

1 Präambel

PROVENTOR entwickelt und betreibt Softwarelösungen für die Dokumentation von Sicherheits- und Wartungsthemen. Diese Softwarelösungen werden als Software as a Service (Cloud Service) betrieben.

Diese Vereinbarung zur Auftragsverarbeitung gilt generell für alle PROVENTOR Kunden. Die Zustimmung zur Auftragsverarbeitung wird gesondert in einer Lizenzvereinbarung mit Bezug auf diese Vereinbarung geregelt.

2 Auftragsverarbeitung gemäß Art. 28 DSGVO

2.1 Gegenstand der Vereinbarung

Gegenstand dieser Vereinbarung ist die Durchführung folgender Aufgaben durch den Auftragsverarbeiter:

- Zurverfügungstellung der PROVENTOR Software
- Serverbetrieb und Hosting des angegebenen Systems
- Wartung und Support der Infrastruktur und der Services

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen des Art. 44 ff. DS-GVO erfüllt sind.

2.2 Art und Zweck der Verarbeitung von Daten

Der Zweck der Datenverarbeitung dient ausschließlich dem Verwendungszweck der Software. Die Daten werden vom Auftragsverarbeiter nur im Sinne des Support- und Wartungsvertrages eingesehen und bearbeitet. Eine Weitergabe oder Zweckentfremdung der Daten ist ausgeschlossen.

2.3 Art der Daten

Folgende Datenkategorien werden verarbeitet, Pflichtfelder des Systems sind fett markiert:

- **Personendaten:** Name, E-Mail Adresse, Passwörter, Adresse und Telefonnummern im Bedarfsfall
- **Bewegungsdaten der Personen:** Protokolleinträge, Aufgaben und Versäumnisse, Zugriffsprotokoll, Protokoll des E-Mail-Versands

2.4 Kategorien betroffener Personen

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

- Mitarbeiterinnen & Mitarbeiter, sowie externe Dienstleister des Verantwortlichen

- ggf. Daten von Kunden und Lieferanten je nach Nutzung

2.5 Dauer der Vereinbarung

Die Vereinbarung ist gebunden an die Lizenzvereinbarung. Die Dauer wird gesondert in der Lizenzvereinbarung geregelt.

2.6 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Verwaltungs- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt. Erhält der Auftragsverarbeiter einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragsverarbeiters eines schriftlichen Auftrages des Auftraggebers.

(3) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO.
Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.

(4) Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen des erteilten Auftrages gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO zu erfüllen.

(5) Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32ff DSGVO insbesondere iVm mit Art 5 Abs. 1 und Abs. 2 DSGVO ergriffen hat und deren Einhaltung regelmäßig kontrolliert und dokumentiert. Es handelt sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme (Einzelheiten siehe Anlage Technische und Organisatorische Maßnahmen).

(6) Mitwirkungspflicht bei Betroffenenrechten: Der Auftragsverarbeiter ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Betroffenenrechte nach Kapitel III der DSGVO (insbesondere Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.

Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(7) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Daten Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragsverarbeiter durchzuführen (sicherzustellen).

(8) Der Auftragsverarbeiter verpflichtet sich den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten zu unterstützen. Dazu gehören insbesondere:

a) Die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(9) Der Auftragsverarbeiter führt ein Verarbeitungsverzeichnis nach Art 30 DSGVO.

(10) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(11) Der Auftragsverarbeiter stellt insbesondere sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO; die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit .

(12) Der Auftragsverarbeiter ist spätestens nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinem Besitz gelangte Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber zu übergeben / in dessen Auftrag datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Wenn der Auftragsverarbeiter die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

(13) Der Auftragsverarbeiter hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

2.7 Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen (TOM) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten
Maßnahmen nicht unterschritten wird. Die technischen und organisatorischen Maßnahmen liegen als Anhang bei. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

2.8 Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt. Dies gilt auch für die Leistungen des Sub-Auftragsverarbeiters gemäß Pkt. 7.

2.9 Sub-Auftragsverarbeiter

Der Auftragsverarbeiter ist befugt folgende Unternehmen als Sub-Auftragsverarbeiter zur unmittelbaren Erbringung einer Dienstleistung hinzuziehen:

- Servicedienstleister: MIT e-solutions GmbH, Kärntner Straße 337, A 8054 Graz
- Infrastrukturprovider: A1 Telekom Austria AG, Marburger Kai 43 – 45, A 8010 Graz
- Software-Entwicklungsdienste: 3DataX GmbH & Co KG, Lambrechtgasse 3/3, 1040 Wien

Die erforderlichen Vereinbarungen zwischen dem Auftragsverarbeiter und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO wurden abgeschlossen.
Jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung durch andere Sub-Auftragsverarbeiter bedarf der vorherigen schriftlichen Genehmigung durch den Auftraggeber.
Es ist sichergestellt, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

3 Geltendes Recht

Diese Vereinbarung unterliegt österreichischem Recht. Gerichtsstand ist das sachlich zuständige Gericht in Graz.

Anhang 1 – Technisch-organisatorische Maßnahmen (TOMs)

Vertraulichkeit

- Zutrittskontrolle (wird über Sub-Auftragsverarbeiter abgedeckt): Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
- Zugangskontrolle: Schutz vor unbefugter Systembenutzung: Kennwörter (Richtlinien: keine Mehrfachverwendung, individuelle Richtlinien, Sperre bei mehrfacher Falscheingabe)
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems: Unterschiedliche Systemrollen einstellbar, spezielle Systemadministrationszugriffe gesondert möglich. Serverzugriff nur eingeschränkt auf Mitarbeiter der Abteilung ICT
- Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden: Mandantenfähigkeit im System, getrennte Datenbanken bei Premium Systemen.
- Klassifikationsschema für Daten: Intern

Integrität

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport: Verschlüsselung beim Aufruf des Systems (HTTPS), keine weitere Datenübertragung vorgesehen.
- Eingabekontrolle: Systemlogbuch für die Protokollierung von Änderungen im System sowie automatische Systemprozesse

Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Tägliche Datensicherung (30 Tage rückwirkend) in anderem, Brandabschnitt, Ausfallssicherheit USV, Rasche Wiederherstellbarkeit;
- Löschungsfristen: Datenlöschung nach Vertragsende.

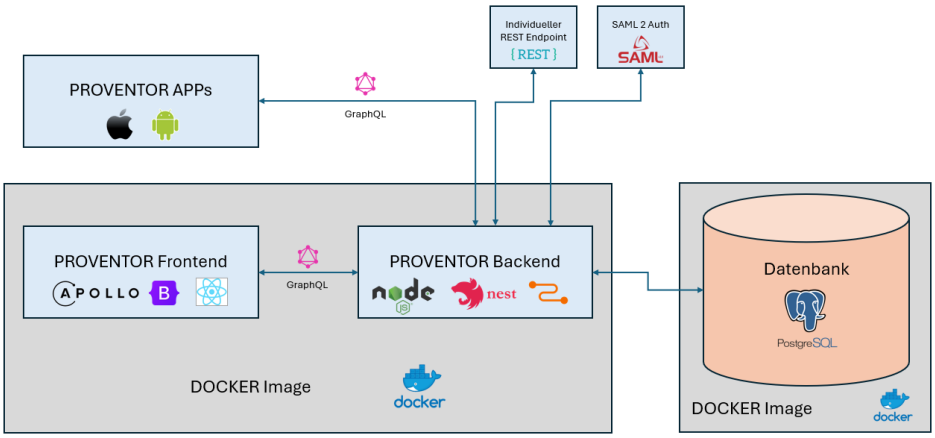
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Hosting & Betrieb der Softwarelösung: Überprüfung der Prozesse und Maßnahmen im Rahmen des jährlichen ISO 9001 Qualitätsaudits (QM). Wiederkehrende (jährliche) Risikoanalysen der Serversysteme inkl. Dokumentation. Forderung der ISO 27001 Zertifizierung des Sub-Auftragsverarbeiters.
- Entwicklung und Wartung der Softwarelösung: Durchführung von umfassenden Sicherheitsüberprüfungen bei jedem Major Release der Software (Version X.1.1), Überprüfung der Einhaltung von Datenschutzrichtlinien bei jedem Minor Release (Version 1.X.1). Definierte Security Richtlinien bei Software-Entwicklung und Kontrolle der Einhaltung durch Code Review Prozess sowie interne und externe ISO 9001 Audits (QM).

Anhang 2 – Sicherheitsinformationen für PROVENTOR Kunden

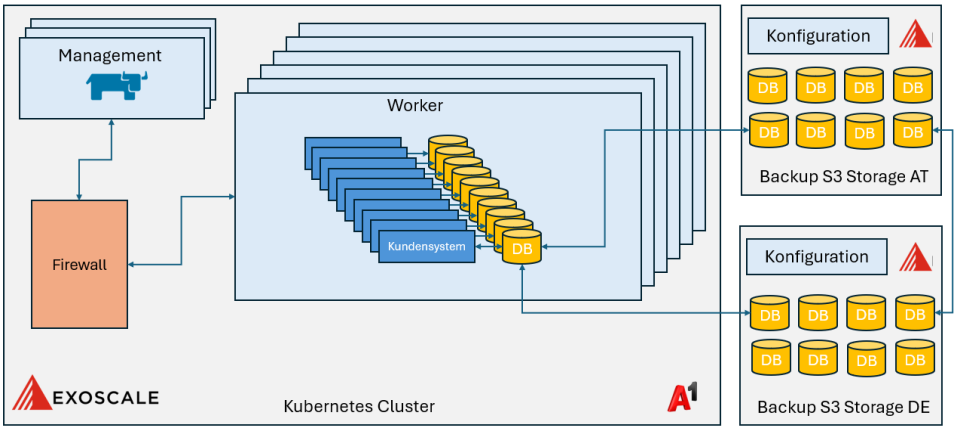
Systemarchitektur

PROVENTOR betreibt ein Web-basiertes Softwaresystem welches aus einer Systemkomponente sowie einer Datenbank besteht. Zusätzlich sind mobile APPs für Android und iOS verfügbar, welche an das System mittel Schnittstelle angedockt sind.



Betriebsarchitektur

Die Kundensysteme werden als DOCKER Images verwaltet und auf einem Kubernetes Cluster betrieben.



Im Kubernetes-Cluster werden einzelne Kundensysteme überwacht und die Verfügbarkeit sichergestellt. Im Falle eines Systemausfalls wird dieses nach 30 Sekunden neu gestartet, fällt ein Worker aus, so werden die Systeme automatisiert auf andere Worker verteilt. Ein manueller Eingriff ist nur selten notwendig, bei einem Komplettausfall des Clusters kann dieser innerhalb von 24 Stunden im Ausfallsrechenzentrum in Betrieb genommen werden, da die Daten in beiden Rechenzentren grundsätzlich vorhanden sind.

Sicherungskonzept

Folgende Basissicherungen werden durchgeführt und verteilt:

- Tägliche Vollsicherung jeder Kundendatenbank (DMP)
- Tägliche inkrementelle Komplettsicherung des gesamten Clusters
- Sicherungen werden am S3 Storage des Rechenzentrums durchgeführt
- Sicherungen werden automatisiert auf einen Ausweichstandort kopiert
- Sicherungen werden einmal wöchentlich auf eine verschlüsselte Festplatte kopiert (2 unterschiedliche Festplatten) und in einem Tresor abgelegt

Durch dieses Sicherungskonzept sind die Kundendaten für Standard- und Desaster Recovery abgesichert. Im unwahrscheinlichen Fall einer Verschlüsselung können auf unterschiedliche Sicherungen bzw. auch die Harddisk Sicherungen zurückgegriffen werden.
Datenwiederherstellungen können kurzfristig (vom Vortag) eingespielt werden. Alle Sicherungen werden 365 Tage rückwirkend gespeichert.
Im Falle einer Vertragsauflösung werden die Daten an den Kunden bei Bedarf übermittelt, und anschließend die Datenbank sowie die Datenbanken in den einzelnen Sicherungen entfernt. Nach der Löschung ist eine Widerherstellung nicht möglich. Datenträger auf denen sich Unternehmensdaten befinden, werden (nach Ausscheiden) zur Vernichtung an eine Fachfirma übergeben.

Datenschutz und Dokumentation

Der Schutz von personenbezogenen Daten ist Teil des gesamten Software- und Betriebskonzeptes von PROVENTOR.

Datenschutz in der Applikation:
In der Applikation PROVENTOR werden nur notwendige personenbezogene Daten gespeichert. Erforderlich sind nur E-Mail-Adresse, Vorname und Nachname der jeweiligen Benutzer. Diese Daten können mit Funktion, Telefonnummer und Standort angereichert werden. Zusätzlich wird für jede Begehung der Zeitpunkt der Durchführung und Eintragung dokumentiert. Das Protokoll in PROVENTOR gilt als rechtssicher, dahingehend ist keine Löschung von Einträgen möglich. Personen können aber anonymisiert werden. Dahingehend stehen 2 Funktionen zur Verfügung:

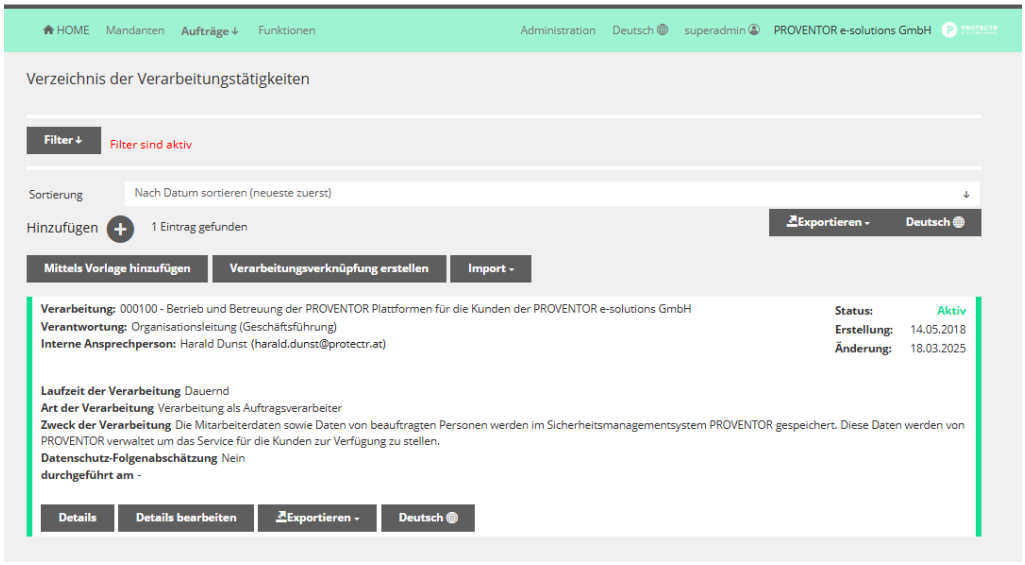
- Teilweise anonymisieren: Alles wird gelöscht, nur der Vorname und der Nachname bleibt erhalten. Dies ist teilweise notwendig, um im rechtssicheren Protokoll die tatsächliche Person nachzuweisen.
- Gänzlich anonymisieren: Alle Daten werden gelöscht bzw. Vorname, Nachname und E-Mail-Adresse mit einem Hash versehen. Dahingehend ist zwar nachvollziehbar, dass eine Begehung durchgeführt wurde, aber nicht von welcher Person

Zusätzlich zu diesen Funktionalitäten steht eine erweiterte Datenauskunftsfunktion zur Verfügung, welche pro Person anzeigt, wo sich überall personenbezogene Daten in der Applikation befinden.
Auch eine Datenübertragung oder ein maschinenlesbarer Gesamt-Datenexport ist möglich, nach Auflösung des Vertrages.

Dokumentation des Datenschutzes bei PROVENTOR

PROVENTOR führt ein Verzeichnis der Verarbeitungstätigkeiten im PROVENTOR Datenschutz System. Für alle Kunden des PROVENTOR Systems wird eine Verarbeitungstätigkeit geführt, bei dem die Kunden als Auftraggeber hinterlegt sind, da der Zweck der Verarbeitung bei allen Kunden gleich ist.

Verarbeitungsverzeichnis in der Software:



Auszug aus dem Verarbeitungsexport:

Verarbeitung 000100

Verarbeitungs-Nr:	000100
Bezeichnung:	Betrieb und Betreuung der PROVENTOR Plattformen für die Kunden der PROVENTOR e-solutions GmbH
Gemeinsame Verarbeitung:	Nein
Beschreibung für die gemeinsame Verarbeitung:	
Datum der Ersterfassung:	14.05.2018
Laufzeit der Verarbeitung:	Dauernd
Art der Verarbeitung:	Verarbeitung als Auftragsverarbeiter
Mehrere Nutzer der Verarbeitung:	Ja
Benachrichtigungsadressen:	
Weitere Anmerkungen zur Verarbeitung:	Mit jedem Kunden in der Liste der Nutzer der Verarbeitung wurde eine Vereinbarung zur Auftragsverarbeitung geschlossen. Diese sind abgelegt am Sharepoint unter "Bestehende Kunden"
Interne Ansprechperson:	Harald Dunst
Besitzer der Daten / Organisationseinheit:	Organisationsleitung (Geschäftsführung)

Auftragsverarbeitung

Firma:	Siehe Nutzer der Verarbeitung
Name:	Siehe Nutzer der Verarbeitung
E-Mail Adresse:	Siehe Nutzer der Verarbeitung
Telefonnummer:	Siehe Nutzer der Verarbeitung
Vertrag gültig bis:	01.01.2030
Datenschutzvereinbarung mit Kunde:	Ja
Adresse:	Adresse: Siehe Nutzer der Verarbeitung PLZ: 8054 Ort: Graz Land: Österreich

Zwecke der Verarbeitung:	Die Mitarbeiterdaten sowie Daten von beauftragten Personen werden im Sicherheitsmanagementsystem PROVENTOR gespeichert. Diese Daten werden von PROVENTOR verwaltet um das Service für die Kunden zur Verfügung zu stellen.
Einwilligung der betroffenen Person:	Nein
Vertragserfüllung:	Ja / Die Daten werden durch bestehende Verträge (oder bei Teststellungen) durch vorvertragliche Maßnahmen gespeichert.
Gesetzliche Verpflichtung:	Nein
Lebenswichtige Interessen:	Nein
Öffentliches Interesse:	Nein
Berechtigtes Interesse:	Nein

Maßnahmen und Empfänger

Informationspflicht erfüllt:	Ja
Beschreibung der Informationspflicht:	Die Informationspflicht für alle Plattformbenutzer wird direkt beim System angezeigt (siehe: https://expert.protectr-app.com/static/U3RhdGljUGFnZToy)
Zweckbindung eingehalten:	Ja
Datenminimierung eingehalten:	Ja
Richtigkeit sichergestellt:	Ja
Löschfristen definiert:	Ja
Interne Empfänger:	
Externe Empfänger:	10 Auftragsverarbeiter (IT Dienstleister, Versanddienstleister, Druckereien, Reisebüros, Inkassounternehmen)

Datenablageort:	Elektronische Datenverarbeitung (manuell)
Bezeichnung der Ablage:	A1 - Exoscale Service / Server: Vienna / Serverhosting - betreuung durch MIT e-solutions GmbH
Beschreibung der Ablage:	Auf den genannten Exoscale Servern werden die einzelnen System von PROTECTR betrieben. EXOSCALE hat keinen direkten Zugriff auf die enthaltenen Daten sondern stellt nur den Speicherplatz sowie die Datensicherheit sichr.
Technische und Organisatorische Maßnahmen:	Interne elektronische Datenverarbeitung auf internen Servern bzw. zur Verfügung gestellten externen Services. Zur Gewährleistung der Zuverlässigkeit, Vertraulichkeit, Verfügbarkeit und Belastbarkeit werden folgende Datensicherheitsmaßnahmen durchgeführt: Zugangs- und Zugriffskontrolle Speicher- und Datenträgerkontrolle Eingabe- und Übertragungskontrolle Wiederherstellung
Verantwortlich:	Harald Dunst

Daten

Datenkategorie	Personenkategorie	Datenquelle	Datenablageort	Besondere Datenkategorie	Speicherdauer / Löschfristen	Externe Empfänger	Interne Empfänger	Zusätzliche Informationen
01 Stammdaten (Akad. Grad, Geschlecht, Vorname, Nachname, Adresse, PLZ, Ort)	02 Kunden bzw. Mitarbeiter von Kunden	01 Vom Betroffenen erhoben/ übermittelt	A1 - Exoscale Service / Server: Vienna / Serverhosting - betreuung durch MIT e-solutions GmbH	Nein	1 Jahr	10 Auftragsverarbeiter (IT Dienstleister, Versanddienstleister, Druckereien, Reisebüros, Inkassounternehmen)		Datenlöschung spätestens 1 Jahr nach Vertragsbeendigung
02 Kontaktdaten (Telefonnummern, E-Mail Adressen, Fax Nummer)	02 Kunden bzw. Mitarbeiter von Kunden	01 Vom Betroffenen erhoben/ übermittelt	A1 - Exoscale Service / Server: Vienna / Serverhosting - betreuung durch MIT e-solutions GmbH	Nein	1 Jahr	10 Auftragsverarbeiter (IT Dienstleister, Versanddienstleister, Druckereien, Reisebüros, Inkassounternehmen)		Datenlöschung spätestens 1 Jahr nach Vertragsbeendigung