

Vereinbarung zur Auftragsverarbeitung

zwischen

dem vom Hauptnutzer vertretenen Unternehmen
(Verantwortlicher, Auftraggeber)

und der

Hekatron Vertriebs GmbH, Brühlmatten 9, 79295 Sulzburg
(Hekatron, Auftragsverarbeiter, Auftragnehmer)

zum Hekatron Mein HPlus Portal <https://www.meinhplus.de>

Stand: 03.05.2019

1. Gegenstand und Dauer des Auftrags

(1) Mein HPlus ist ein Online-Portal zur Verwaltung und Dokumentation von gebäudetechnischen Anlagen. Das Tool ermöglicht dem Auftraggeber, den Einsatz von Material und Personal zu planen, Wartungen durchzuführen und mittels Analysen zu optimieren.

(2) Diese Vereinbarung bezieht sich auf personenbezogene Daten und ist Teil der Nutzungsbedingungen des Mein HPlus Portals. Der Auftraggeber wird vertreten durch den Hauptnutzer. Nur er kann Weisungen im Sinne dieser Vereinbarung erteilen. Diese sind an die in den Nutzungsbedingungen genannte Stelle zu richten.

(3) Das Portal wird nur als Standard-Dienstleistung angeboten. **Der Auftraggeber darf die Vereinbarung nur annehmen, wenn ihm die in dieser Vereinbarung und ihrer Anlage TOM dargestellten Maßnahmen hinsichtlich Datenschutz und IT-Sicherheit ausreichen.**

(4) Die Vereinbarung tritt mit Wirksamwerden der Nutzungsbedingungen in Kraft, nach Freischaltung des Firmenaccounts im Portal. Sie endet durch Löschen des Firmenaccounts im Portal. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

(5) Sie endet ferner, wenn Hekatron die Dienstleistung nicht fortführen kann, z.B. aufgrund einer Weisung, die im Rahmen der Standard-Dienstleistung nicht mit vertretbarem Aufwand umsetzbar ist. Gleiches gilt bei Widerspruch des Auftraggebers wegen neuer Unterauftragnehmer.

2. Datenverarbeitung im Rahmen des Auftrags

(1) Mit dem Portal kann der Auftraggeber seine Portalnutzer, Kunden und deren Objekte verwalten. Personenbezogene Daten sind auf Kontaktdaten der beteiligten Ansprechpartner beschränkt. Zusätzlich können anlagenbezogene Dokumente hochgeladen werden. Diese werden von Hekatron nur für Support und Fehlersuche eingesehen.

(2) Vom Auftraggeber eingegebene Kontaktdaten seiner Portalnutzer werden mit der Hekatron Kundendatenbank abgeglichen. Hierdurch gewährleistet Hekatron deren Richtigkeit und ermöglicht den Zugriff auf lizenzpflichtige Inhalte und Funktionen.

(3) Zur Aufrechterhaltung des sicheren Betriebs des Portals und zu dessen Verbesserung wird die Nutzung protokolliert. Diese Daten stehen nur Hekatron zur Verfügung, werden von Hekatron dauerhaft gespeichert, aber nur in aggregierter oder anonymisierter Form genutzt.

(4) Die Kategorien der durch die Verarbeitung betroffenen Personen und die Arten der jeweils über sie verwendeten personenbezogenen Daten umfassen:

Kundendaten (Ansprechpartner der Kunden des Auftraggebers)

- Stammdaten, z.Zt.: Name, E-Mail, Telefon, Zuordnung zur Anlage, Firma, Position/Funktion
- Dokumentenablage: beliebige Dateien mit Bezug zur Anlage

Portalnutzer (Mitarbeiter des Auftraggebers)

- Stammdaten, z.Zt.: Name, Benutzername, Initialpasswort/Passwort-Hash, E-Mail, Telefon, Firma, Rolle/Rechte im Portal
- Servicedaten, z.Zt.: Planung/Durchführung, Liegenschaft/Anlage, Start/Ende
- Protokolle, z.Zt.: Anmeldezeitpunkt, Nutzung der Portalfunktionen inkl. Zeitpunkt

(5) Das Portal stellt Funktionen zur Verfügung, mit denen der Auftraggeber alle Daten seiner Kunden und Portalnutzer selbst verwalten kann: Von der Anlage über die Korrektur und den Export bis hin zur Sperrung und Löschung. Hekatron wird nur auf explizite Weisung des Auftraggebers tätig.

3. Pflichten des Auftragnehmers

(1) Hekatron darf personenbezogene Daten nur im Rahmen der vereinbarten Dienstleistung oder auf explizite Weisung des Auftraggebers verarbeiten. Gesetzliche Pflichten sind davon unbenommen. Sicherheitskopien zur Gewährleistung der ordnungsgemäßen Datenverarbeitung sind erlaubt.

(2) Hekatron informiert den Auftraggeber unverzüglich, wenn Hekatron der Meinung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Hekatron darf die Durchführung dieser Weisung so lange aussetzen, bis sie durch den Auftraggeber bestätigt oder abgeändert wird.

(3) Hekatron setzt für den Auftrag nur Beschäftigte ein, die zuvor im Datenschutz unterwiesen und auf Vertraulichkeit verpflichtet wurden. Hekatron hat einen Datenschutzbeauftragten benannt. Er kann vom Auftraggeber und betroffenen Personen kontaktiert werden: datenschutz@hekatron.de.

(4) Hekatron hält alle einschlägigen Datenschutzbestimmungen ein und setzt alle vereinbarten technischen und organisatorischen Maßnahmen um. Hekatron kontrolliert die internen Prozesse und technischen und organisatorischen Maßnahmen regelmäßig hinsichtlich der Anforderungen des Datenschutzrechts. Hekatron gewährleistet die Nachweisbarkeit der getroffenen Maßnahmen im Rahmen der Kontrollbefugnisse des Auftraggebers.

(5) Hekatron und der Auftraggeber arbeiten auf Anfrage mit der zuständigen Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Bezogen auf diese Auftragsverarbeitung informieren sie sich gegenseitig über Kontrollen der Aufsichtsbehörde, anhängige Verfahren und sonstige Ansprüche.

(6) Hekatron unterstützt den Auftraggeber bei dessen Informationspflicht gegenüber betroffenen Personen. Sofern der Auftraggeber eine Datenschutz-Folgenabschätzung durchführt oder die Aufsichtsbehörde diesbezüglich konsultiert, unterstützt ihn Hekatron auch dabei.

(7) Nach Abschluss des Auftrags oder nach Aufforderung durch den Auftraggeber händigt Hekatron alle verarbeiteten personenbezogenen Daten aus. Alternativ vernichtet Hekatron die Daten nach Zustimmung durch den Auftraggeber datenschutzgerecht.

(8) Hekatron bewahrt Nachweise für die auftragsgemäße und ordnungsgemäße Datenverarbeitung entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus auf. Hekatron kann diese Nachweise zur eigenen Entlastung dem Auftraggeber übergeben.

4. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung der in dieser Vereinbarung zugesicherten Maßnahmen im laufenden Betrieb zu überzeugen. Die Prüfer sind vom Auftraggeber im Einzelfall zu benennen.

(2) Für die Ermöglichung von Kontrollen kann Hekatron eine Vergütung verlangen, wenn Hekatron zuvor unaufgefordert einen Nachweis über die Einhaltung der Datenschutzvorschriften und vereinbarten Maßnahmen erbracht hat, der Auftraggeber aber dennoch eine eigene Stichprobenkontrolle durchführt.

(3) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens in Textform).

(4) Nur der Auftraggeber nimmt die Rechte der betroffenen Personen wahr. Soweit sich eine betroffene Person bezüglich ihrer Rechte an Hekatron wendet, wird dieses Ersuchen unverzüglich an den Auftraggeber weitergeleitet.

5. Ort der Leistungserbringung und Unterauftragnehmer

(1) Ein Unterauftrag im Sinne dieser Vereinbarung ist eine Dienstleistung, die sich unmittelbar auf die Erbringung der Hauptleistung bezieht. Ein Unterauftrag setzt voraus, dass eine entsprechende Vereinbarung zwischen Hekatron und dem Unterauftragnehmer geschlossen wurde.

(2) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu:

Firma	Leistung
Securiton AG, Alpenstraße 20, CH-3052 Zollikofen	Portal-Betrieb: Infrastruktur, Server
Schrack Seconet AG, Eibesbrunnnergasse 18, A-1120 Wien	Portal-Betrieb: Anwendung, Support

(3) Hekatron kann weitere Unterauftragnehmer beauftragen oder bestehende ersetzen. In diesem Fall informiert Hekatron den Auftraggeber hierüber rechtzeitig vorab.

(4) Erhebt der Auftraggeber Einspruch gegen den Einsatz eines neuen Unterauftragnehmers, so kann Hekatron die Dienstleistung nicht fortführen. Dies stellt eine fristgerechte ordentliche Kündigung dar.

(5) Die Datenverarbeitung findet zurzeit ausschließlich in Deutschland, Österreich und der Schweiz statt. Hekatron darf die Datenverarbeitung in ein anderes Land des europäischen Wirtschaftsraums verlagern, muss den Auftraggeber aber rechtzeitig vorab informieren. Die Verlagerung in ein Drittland ist nur nach vorheriger Zustimmung des Auftraggebers zulässig.

(6) Eine Unterbeauftragung durch den Unterauftragnehmer bedarf der Zustimmung von Hekatron.

6. Technische und organisatorische Maßnahmen

(1) Hekatron gewährleistet die Sicherheit der Datenverarbeitung. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es Hekatron gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Anlage TOM – Technische und organisatorische Maßnahmen

Diese Anlage fasst die wesentlichen technischen und organisatorischen Maßnahmen von Hekatron als **Anbieter und Betreiber**, von Schrack Seconet als **Entwicklungs- und Technikpartner** sowie der SOP als **Infrastruktur-Provider** zusammen. Die Maßnahmen dienen dazu, Datenschutzvorschriften zu erfüllen und die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten zu gewährleisten.

Rechenzentrum

Das gesamte Anwendungssystem Mein HPlus inklusive Ihrer Daten wird in einem Rechenzentrum in der Schweiz betrieben. Dieses Rechenzentrum ist gemäß Tier-IV-Standard gebaut und nach ISO 27001 zertifiziert, so dass höchste Sicherheits- und Verfügbarkeitsstandards erfüllt werden.

Cloud-Plattform

Ihre Daten liegen in einer Datenbank in einem eigenen, separaten Bereich des Rechenzentrums. Dieser wird als SOP (Secure-Online-Plattform) bezeichnet und von der Securiton AG betrieben. Die SOP ist eine modular aufgebaute private Cloud mit zentralen Firewalls, strikter Mandantentrennung (Multi-Tenancy), redundanter Infrastruktur mit automatisierten Backups sowie 24/7-Monitoring.

Applikation

Die Anwendung Mein HPlus besteht aus einer Web-Anwendung und einer Datenbank. Sie basiert auf langjährig erprobten Komponenten, die gemeinsam mit Schrack Seconet und erfahrenen Software-Entwicklungspartnern entwickelt, getestet und administriert werden. Datenübertragungen erfolgen stets über verschlüsselte Verbindungen (TLS 1.2).

Zugriffsrechte

Das Portal ist hierarchisch aufgebaut und bietet ein Rollenkonzept. Nutzer haben nur Zugriff auf die eigene Organisationseinheit und die darunter liegenden. Hekatron legt je Organisationseinheit einen Hauptnutzer an. Dieser ist Administrator und kann weitere Portalnutzer (Nebennutzer) anlegen. Jedem Nutzer ist eine Rolle (Administrator, Projektleiter, Techniker) zugeordnet. Hiermit kann der Zugriff auf einzelne Projekte granular gesteuert werden.

Nutzer-Zugang

Portalnutzer müssen sich mit Benutzernamen, Passwort und zweitem Faktor anmelden (TOTP).

Server-Administration

Der Zugriff auf die Server ist nur den Systemadministratoren der Hekatron, Schrack Seconet und Securiton möglich. Er erfolgt über VPN-Verbindungen mit 2-Faktor-Authentifizierung. Jede Anmeldung wird protokolliert. Alle Systemadministratoren und Supportmitarbeiter sind im Datenschutz unterwiesen und zur Wahrung der Vertraulichkeit verpflichtet.

Kunden-Support

Der Hekatron Kundensupport hat Benutzerkonten mit erweiterten Rechten. Diese ermöglichen den Datenzugriff im Support- bzw. Fehlerfall. Die Supportorganisation ist in Ebenen (Support-Level) aufgeteilt, die jeweils nur den auf dieser Ebene notwendigen Zugriff haben. Der Support sichtet und ändert Daten nur nach explizitem Auftrag.