Vereinbarung zur Auftragsverarbeitung

zwischen

die vom Hauptnutzer vertretene Organisation
(Verantwortliche, Auftraggeberin)

und

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

Stand: 07.12.2022

1. Kontext und Vorbedingungen

(a) Das digitale Hekatron-Produkt Mein HPlus besteht aus einem Online-Portal (Mein HPlus Service-Portal) und mobilen Apps (Mein HPlus Service-App) zur Verwaltung und Dokumentation gebäudetechnischer Anlagen. Es wird als „digitales Produkt“ bezeichnet. Das digitale Produkt ermöglicht der Auftraggeberin, den Einsatz von Material und Personal zu planen, Wartungen durchzuführen und mittels Analysen zu optimieren.

(b) Diese Vereinbarung bezieht sich auf die Verarbeitung personenbezogener Daten im digitalen Produkt und ist Teil der Nutzungsbedingungen von Mein HPlus Service-Portal/-App. Das digitale Produkt wird nur als Standard-Dienstleistung angeboten. **Die Auftraggeberin darf die Vereinbarung nur annehmen, wenn ihr die in dieser Vereinbarung und der zugehörigen Anlage TOM dargestellten Maßnahmen hinsichtlich Datenschutz und IT-Sicherheit ausreichen.**

(c) 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 der Auftraggeberin wegen neuer Unterauftragnehmer.

2. Beginn, Dauer und Gegenstand des Auftrags

(a) Diese Vereinbarung gilt, sobald und solange die Auftraggeberin den digitalen Dienst in Anspruch nimmt. Sie kann durch Löschen des Firmen-Accounts beendet werden. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

(b) Mit dem digitalen Produkt kann die Auftraggeberin ihre Portalnutzer, Kunden und deren Objekte verwalten. Personenbezogene Daten sind primär Kontaktdaten der beteiligten Ansprechpartner und gegebenenfalls Unterschriften auf Wartungsprotokollen. Zusätzlich können anlagenbezogene Dokumente hochgeladen werden. Alle Daten werden von Hekatron nur für Support und Fehlersuche eingesehen.

Von der Auftraggeberin eingegebene Kontaktdaten ihrer Portalnutzer werden mit der Hekatron Kundendatenbank abgeglichen. Hierdurch gewährleistet Hekatron deren Richtigkeit und ermöglicht den Zugriff auf lizenzpflichtige Inhalte und Funktionen.

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.

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

Kundendaten (Ansprechpartner der Kunden der Auftraggeberin)

- Stammdaten: Name, E-Mail, Telefon, Zuordnung zur Anlage, Firma, Position/Funktion
- Protokolle: Unterschriften in Tätigkeitsnachweisen
- Dokumentenablage: beliebige Dateien mit Bezug zur Anlage

Portalnutzer (Mitarbeiter des Auftraggebers)

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

Die hinter den Kategorien aufgeführten Datenfelder dienen dem Verständnis und können erweitert werden.

(d) Das digitale Produkt stellt Funktionen zur Verfügung, mit denen die Auftraggeberin alle Daten ihrer Kunden und Portalnutzer selbst verwalten kann: Von der Anlage über die Korrektur und den Export bis hin zur Sperrung und Löschung. Hekatron wird bzgl. Kundendaten nur auf explizite Weisung der Auftraggeberin tätig.

3. Ort der Leitungserbringung und Unterauftragnehmer

(a) Ein Unterauftrag im Sinne dieser Vereinbarung ist eine Dienstleistung, die sich unmittelbar auf die Erbringung der Hauptleistung bezieht. Er setzt voraus, dass Hekatron eine Vereinbarung zur Auftragsverarbeitung mit dem Unterauftragnehmer geschlossen hat.

(b) Die Auftraggeberin stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu:

- Hosting (Infrastruktur, Server) durch Securitas AG, Alpenstraße 20, 3052 Zollikofen, Schweiz
- Entwicklung (Support) durch hard&softWERK GmbH, Bahnhofstraße 10, 78112 St. Georgen
- Application Management (24/7) & Support durch diva-e Cloud GmbH, Mälzerstraße 3, 07745 Jena

Eine weitere Unterbeauftragung durch den Unterauftragnehmer bedarf der Zustimmung von Hekatron.

(c) Hekatron kann weitere Unterauftragnehmer beauftragen oder bestehende ersetzen, sofern die Auftraggeberin rechtzeitig vorab informiert wird. Erhebt die Auftraggeberin Einspruch gegen den Einsatz eines neuen Unterauftragnehmers, so kann Hekatron die Dienstleistung nicht fortführen. Dies stellt eine fristgerechte ordentliche Kündigung dar.

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

4. Technische und organisatorische Maßnahmen

(a) Hekatron hält die in Anlage TOM beschriebenen technischen und organisatorischen Maßnahmen ein. Diese reichen aus Sicht der Vertragsparteien aus, um das Risiko für die Betroffenen bzgl. deren Grundrechte und Grundfreiheiten bei der Verarbeitung ihrer Daten auf ein für sie akzeptables Maß zu beschränken.

(b) Hekatron überprüft die Wirksamkeit der Maßnahmen regelmäßig und weist diese auf Anfrage nach. Stellt Hekatron fest, dass diese nicht mehr ausreichen, informiert Hekatron die Auftraggeberin und passt die Maßnahmen im Einvernehmen an. Hierdurch entstehende Mehraufwände sind zu verhandeln.

5. Pflichten von Hekatron

(a) Hekatron weist der Auftraggeberin die Einhaltung einschlägiger Datenschutzbestimmungen auf Anfrage nach und unterstützt die Auftraggeberin bei der Erfüllung der Betroffenenrechte sowie bei Meldungen bzw. Benachrichtigungen im Falle von Datenschutzverletzungen. Hekatron gewährleistet, dass festgestellte Datenschutzverletzungen bezüglich der o.g. Daten unverzüglich an die Auftraggeberin gemeldet werden.

(b) Hekatron setzt zur Durchführung des Auftrags nur Beschäftigte ein, die mit den relevanten Bestimmungen zum Datenschutz vertraut sind und auf Vertraulichkeit verpflichtet wurden. Hekatron gewährleistet, dass sie und ihre Beschäftigten die oben genannten Daten nur so verarbeiten, wie es der erteilte Auftrag erfordert, aufgrund einer konkreten Weisung der Auftraggeberin oder soweit Hekatron gesetzlich zur Verarbeitung der Daten verpflichtet ist.

6. Weisungsbefugnis und Kontaktdaten

(a) Die Auftraggeberin wird vertreten durch ihren Hauptnutzer. Nur er kann Weisungen im Sinne dieser Vereinbarung erteilen. Diese sind an die in den Nutzungsbedingungen genannte Stelle zu richten. Mündliche Weisungen müssen von der Auftraggeberin mindestens in Textform bestätigt werden.

(b) Hekatron informiert die Auftraggeberin unverzüglich, wenn Hekatron der Meinung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Hekatron ist berechtigt, die Durchführung dieser Weisung so lange auszusetzen, bis sie durch die Auftraggeberin bestätigt oder geändert wird.

(c) Hekatron hat einen Datenschutzbeauftragten benannt. Er kann von der Auftraggeberin und von betroffenen Personen direkt kontaktiert werden. Er ist per E-Mail erreichbar unter datenschutz@hekatron.de.

Die Auftraggeberin gewährleistet, dass die Kontaktdaten der für den Datenschutz verantwortlichen Personen sowie – sofern benannt – des/der Datenschutzbeauftragten Hekatron bekannt sind.

7. Kontrollrechte der Auftraggeberin

(a) Die Auftraggeberin hat das Recht, sich durch angemeldete Kontrollen von der Einhaltung dieser Vereinbarung im Geschäftsbetrieb zu überzeugen. Die Prüfer*innen sind von der Auftraggeberin im Einzelfall zu benennen.

(b) Hekatron kann die Einhaltung der Vorschriften und Maßnahmen auch durch ein geeignetes Zertifikat eines unabhängigen Sachverständigen nachweisen. Verlangt die Auftraggeberin trotz gültigem Zertifikat eine eigene Kontrolle, kann Hekatron für entstandenen Mehraufwand eine Vergütung verlangen.

8. Löschung und Rückgabe von Daten

(a) Ohne das Wissen der Auftraggeberin dürfen keine Daten aus dem digitalen System kopiert werden. Ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung, sowie Daten, die gelöscht werden sollen, für die aber noch gesetzliche Aufbewahrungspflichten gelten.

(b) Nach Abschluss des Auftrags oder nach Aufforderung durch die Auftraggeberin hat Hekatron alle in ihren Besitz gelangten personenbezogenen Daten auszuhändigen oder – nach vorheriger Zustimmung durch die Auftraggeberin – datenschutzgerecht zu vernichten und dies zu protokollieren.

(c) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind von Hekatron entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Sie kann sie zu ihrer Entlastung an die Auftraggeberin übergeben.

Anlage TOM: Technische und organisatorische Maßnahmen

Dies beinhaltet die wesentlichen technischen und organisatorischen Maßnahmen von Hekatron als Anbieter und Betreiber, von hard&softWERK als Entwicklungspartner, von diva-e als Application Management Partner sowie Securitas für Hosting und zentrale Dienste.

Rechenzentrum: Das digitale Produkt Mein HPlus wird in einem Rechenzentrum in der Schweiz betrieben. Es entspricht Tier-IV Standard und ist ISO 27001 zertifiziert, so dass höchste Sicherheits- und Verfügbarkeitsstandards erfüllt werden.

Cloud-Plattform: Die Daten liegen in einem zugangsgesicherten Bereich des Rechenzentrums, der SOP (Secure-Online-Plattform). Die SOP ist eine modular aufgebaute private Cloud und wird von der Securitas AG betrieben.

Die SOP stellt eine redundante Infrastruktur, Tenants für Gruppengesellschaften und Applikationen und zentrale Dienste bereit, z.B. Server, Storage, Datenbanken, Firewall/IDS, ID-Management, automatisierte Backups und 24/7-Monitoring. Der Betrieb der SOP-Cloud-Infrastruktur durch die Securitas AG ist ebenfalls nach ISO 27001 zertifiziert.

Applikation: Das digitale Produkt besteht aus einer Web-Anwendung, einer Datenbank und mobilen Apps (Android/iOS). Es werden langjährig erprobte Komponenten verwendet, die gemeinsam mit erfahrenen Partnern entwickelt und getestet werden. Hekatron administriert das Produktivsystem selbst sowie mit Unterstützung des Entwicklungspartners hard&softWERK und des Application Management Partners diva-e.

Datenübertragungen erfolgen stets über verschlüsselte Verbindungen (TLS 1.3 sofern unterstützt, sonst TLS 1.2). Die Anwendung wird basierend auf einem IT-Sicherheitskonzept entwickelt und betrieben. Dieses wird durch externe Sicherheitsfirmen überprüft (bspw. mittels Penetration-Tests).

Zugriffsrechte: Das digitale Portal bietet ein Rollenkonzept. Nutzer haben nur Zugriff auf die eigene Organisationseinheit. Je Organisationseinheit wird ein Hauptnutzer angelegt. Dieser ist bezüglich des Firmen-Accounts Administrator und kann weitere Portalnutzer (Nebennutzer) anlegen. Jedem Nutzer ist eine Rolle (Administrator, Innendienst, Techniker) zugeordnet. Über die Rolle eines Nutzers wird gesteuert, welche Funktionen und Informationen er nutzen darf.

Nutzer-Zugang: Portalnutzer müssen sich mit Benutzername/E-Mail-Adresse und Passwort anmelden. Jeder Nutzer hat die Möglichkeit eine Zwei-Faktor-Authentifizierung (2FA/TOTP) zu aktivieren.

Server-Administration: Der Zugriff auf die Server ist nur den Systemadministratoren von Hekatron und im Rahmen eine Unterauftragsverarbeitungsverhältnisses den Systemadministratoren von diva-e als Application Management Partner (24/7 Monitoring und Betrieb sowie betriebsnaher Support) erlaubt.

Des Weiteren ist der Server-Zugriff – auf expliziten Auftrag seitens Hekatron – auch von hard&softWERK im Rahmen von Software-Deployments, Kunden-Support, System-Konfiguration und Datenbearbeitung erlaubt.

Seitens Securitas findet keine direkte Bearbeitung der Daten statt, eine Einsicht auf die Daten durch Systemadministratoren ist jedoch im Rahmen von Infrastruktur-Arbeiten (z.B. Konfiguration/Backup) möglich. Die Zugriffe der Systemadministratoren erfolgen stets über VPN-Verbindungen mit Zwei-Faktor-Authentifizierung (2FA). Jede VPN-An- bzw. - Abmeldung auf die SOP-Infrastruktur durch die Systemadministratoren wird protokolliert. Alle Systemadministrationen und Supportmitarbeiter sind im Daten-schutz unterwiesen und auf das Datengeheimnis verpflichtet.

Kunden-Support: Die Support-Organisation des Hekatron Kundensupports ist in Ebenen (Support-Level) aufgeteilt, die jeweils nur den auf dieser Ebene notwendigen Zugriff haben. Nur der 3rd-Level-Support hat über Systemadministratoren direkten Zugriff auf die Server, um den Datenzugriff im Support- bzw. Fehlerfall zu ermöglichen. Der Support sichtet und ändert Daten nur nach explizitem Auftrag.

Überprüfung und Verbesserung: Es wird regelmäßig geprüft, ob sich durch technischen Fortschritt neue Risiken und Möglichkeiten der besseren Absicherung ergeben. Gegebenenfalls werden diese Maßnahmen angepasst und Änderungen dokumentiert.
