Vereinbarung zur

Verarbeitung personenbezogener Daten im Auftrag

zwischen dem
vom Hauptnutzer vertretenen Unternehmen (Auftraggeber)
und der
Hekatron Vertriebs GmbH, Brühlmatten 9, 79295 Sulzburg (Hekatron)
als Auftragnehmer

Stand: 30.04.2021

Diese Vereinbarung bezieht sich auf den Vertrag zur Nutzung des Systems Genius Plus gemäß den „Nutzungsbedingungen für die Apps Genius Home / Genius Pro und für die Genius Web Services“ (Hauptvertrag).

1 Gegenstand der Vereinbarung

1.1 Hekatron bietet das technische System Genius Plus als standardisierte Dienstleistung mit zentraler Datenhaltung für seine Partner und Kunden an. Hauptfunktionen des Systems sind die Unterstützung bei der Durchführung der Inbetriebnahme und Wartung von Rauchwarnmeldern sowie deren intelligente Vernetzung.

In diesem Rahmen verarbeitet Hekatron auch personenbezogene Daten im Auftrag des Auftraggebers. Die Entwicklung und den Betrieb des Systems beauftragt Hekatron bei einem Anbieter für mobile Apps und internetbasierte Datendienste (Betreiber).

Da die Dienstleistung nur standardisiert für alle Kunden von Hekatron angeboten wird, kann der Auftraggeber keine individuellen Bedingungen mit Hekatron verhandeln. Der Auftraggeber darf die Vereinbarung daher nur annehmen, wenn ihm die hier angebotenen Maßnahmen hinsichtlich Datenschutz und IT-Sicherheit ausreichen.

1.2 Der Auftrag bezieht sich auf das System Genius Plus, das derzeit folgende Komponenten umfasst:

- Genius Plus: Rauchwarnmelder mit akustischer Datenübertragung
- Genius App: Erfassung des Zustands der Rauchwarnmelder
- Genius Web: Oberfläche zur Verwaltung im Browser
- Genius Cloud: Plattform zur Synchronisation im Rechenzentrum

1.3 Umfang, Art und Zweck der Datenerhebung, -verarbeitung und -nutzung:

- Verwaltung der Zugänge für Nutzer (Mitarbeiter des Auftraggebers) und ihnen zugeordnete Geräte
- Verwaltung der Kunden des Auftraggebers (Wartungsnehmer) und der zu wartenden Liegenschaften
- Durchführen von Wartungen: Erfassung der Melderdaten, Dokumentation der Umstände (Text, Foto), Zuordnung zum Wartungstechniker, zur Liegenschaft und zum Wartungsnehmer

1.4 Art der Daten je Kreis der Betroffenen:

- Mitarbeiter des Auftraggebers: Name, E-Mail-Adresse, Passwort
- Ansprechpartner beim Wartungsnehmer und in der Liegenschaft: Name, E-Mail-Adresse, Telefonnummer

2 Rechte und Pflichten des Auftraggebers

2.1 Für die Beurteilung der Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber verwaltet alle Daten selbst und kann diese löschen, z.B. Wartungsnehmer, Liegenschaften, Ansprechpartner, Servicetechniker, Wartungen.

2.2 Aufgrund der standardisierten Dienstleistung kann der Auftraggeber keine ergänzenden Weisungen zu Zweck, Art und Umfang der Verarbeitung von Daten erteilen. Hekatron nimmt jedoch Änderungswünsche entgegen und berücksichtigt diese gegebenenfalls bei der Fortentwicklung des Produkts.

In diesem Sinne ist beim Auftraggeber nur der Hauptnutzer weisungsberechtigt. Weisungsempfänger bei Hekatron ist der Hekatron Genius-Support, der per E-Mail unter genius-support@hekatron.de erreichbar ist.

2.3 Der Auftraggeber überprüft die Einhaltung der in Anlage 1 vereinbarten Maßnahmen. Stellt er dabei Fehler oder Unregelmäßigkeiten oder mögliche Sicherheitslücken im System fest, informiert der Auftraggeber Hekatron unverzüglich.

2.4 Der Auftraggeber behandelt Geschäftsgeheimnisse zum System Genius Plus (wie z.B. Schwachstellen oder Datensicherheitsmaßnahmen) vertraulich und gibt sie nur nach Freigabe durch Hekatron an Dritte weiter.

3 Rechte und Pflichten von Hekatron

3.1 Hekatron verarbeitet personenbezogene Daten ausschließlich im Rahmen der gesetzlichen Vorschriften und in der in dieser Vereinbarung festgelegten Art und Weise. Hekatron verwendet die überlassenen Daten für keine

anderen Zwecke und führt die verarbeiteten Daten nicht mit anderen eigenen Datenbeständen zusammen.

3.2 Auf Anfrage teilt Hekatron dem Auftraggeber alle Angaben mit, die er für sein Verfahrensverzeichnis bzw. sein Verzeichnis der Verarbeitungstätigkeiten und seine Datenschutzfolgeabschätzung benötigt. Hekatron unterstützt den Auftraggeber zu den üblichen Geschäftszeiten bei der Durchführung seiner Kontrollen, insbesondere durch Auskünfte. Bei gegebenem Anlass kann der Auftraggeber beim Betreiber Einsicht in die in seinem Auftrag verarbeiteten Daten und deren Verarbeitung (Technik, Prozesse) erhalten.

3.3 Hekatron gewährleistet bei der Vergabe eines Auftrags zur Verarbeitung der personenbezogenen Daten des Auftraggebers, dass die hier vereinbarten Regelungen auch gegenüber dem Unterauftragnehmer gelten.

Die Securiton AG, Zollikofen/Schweiz (Provider) stellt eine Cloud-Infrastruktur im Rechenzentrum in Zürich/Schweiz zur Verfügung. In dieser privaten Cloud der Securitas-Gruppe betreibt die diva-e Cloud GmbH, Frankfurt a. M. (Betreiber) das System.

Weitere Unterauftragnehmer sind nicht geplant. Hekatron kann Unterauftragnehmer jedoch ohne die Zustimmung durch den Auftraggeber beauftragen und wechseln. Auf Anfrage lässt Hekatron dem Auftraggeber eine Liste der Unterauftragnehmer zukommen.

3.4 Außer zur Gewährleitung des ordnungsgemäßen Betriebs werden ohne Wissen des Auftraggebers keine Daten kopiert. Hekatron überprüft regelmäßig anhand von Protokollen und durch unabhängige Sachverständige, ob die mit dem Betreiber vereinbarten Prozesse und die von ihm gewährleisteten Maßnahmen eingehalten werden.

3.5 Die Verarbeitung der Daten findet derzeit ausschließlich in Deutschland und in der Schweiz statt. Hekatron darf die Daten ohne Genehmigung durch den Auftraggeber auch innerhalb der EU verarbeiten (lassen).

3.6 Hekatron hat keinen Zugriff auf Kundendaten. Daher berichtigt Hekatron keine Daten, lässt sie aber löschen oder sperren, wenn der Auftraggeber dies verlangt. Bei Vertragsende löscht Hekatron alle in seinen Besitz gelangten personenbezogenen Daten datenschutzgerecht und bestätigt dies dem Auftraggeber auf Anfrage schriftlich.

4 Datengeheimnis und Datensicherheit

4.1 Hekatron befolgt die einschlägigen datenschutzrechtlichen Vorschriften. Deren Einhaltung wird durch den betrieblichen Datenschutzbeauftragten

überwacht. Derzeit ist Herr Olav Seyfarth zum Datenschutzbeauftragten bestellt. Auf Anfrage teilt Hekatron den aktuell bestellten Datenschutzbeauftragten mit.

Anschrift: Datenschutzbeauftragter
Hekatron Vertriebs GmbH
Brühlmatten 9
79295 Sulzburg

Telefon: +49 7634 500 344

E-Mail: datenschutz@hekatron.de
http://www.hekatron.de/pgp_schluessel/
datenschutz@hekatron.de_(0x8FF7D4E4).asc.zip

4.2 Hekatron gewährleistet, dass alle Mitarbeiter, die personenbezogene Daten verarbeiten, mit den einschlägigen Bestimmungen des Datenschutzes vertraut und schriftlich auf das Datengeheimnis verpflichtet sind.

4.3 Betroffene, deren Daten von Hekatron im Auftrag des Auftraggebers verarbeitet werden, haben ein Recht auf Auskunft. Hekatron erteilt Auskünfte an Betroffene oder Dritte nur, wenn der Auftraggeber dies verlangt oder es eine gesetzliche Verpflichtung hierzu gibt.

4.4 Hekatron setzt die gesetzlich vorgeschriebenen und die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen um und passt sie dem Stand der Technik an. Erhält Hekatron Kenntnis von Störungen oder Sicherheitslücken, veranlasst Hekatron deren unverzügliche Behebung. Kann das vereinbarte Sicherheitsniveau nicht aufrechterhalten werden, teilt Hekatron dies dem Auftraggeber unverzüglich mit.

4.5 Verstößt Hekatron, ein von ihr mit der Verarbeitung betrauter Mitarbeiter oder ein Unterauftragnehmer gegen die hier getroffenen Festlegungen oder datenschutzrechtliche Bestimmungen, so informiert Hekatron den Auftraggeber unverzüglich und umfassend. Gleiches gilt bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten.

5 Beginn, Kündigung, Haftung, Eigentum

5.1 Die Vereinbarung tritt mit der Freischaltung des Hauptnutzers in Kraft. Die Laufzeit der Vereinbarung richtet sich nach der Laufzeit des Hauptvertrags, d.h. bei Beendigung des Hauptvertrags endet auch diese Vereinbarung.

Kann oder möchte Hekatron Anforderungen oder Weisungen des Auftraggebers nicht erfüllen, muss die Vereinbarung gekündigt werden.

5.2 Der Auftraggeber kann die Vereinbarung fristlos aus wichtigem Grund kündigen, wenn Hekatron schwerwiegend gegen ihre Pflichten verstößt oder die gewährten Kontrollrechte verweigert.

Hekatron kann die Vereinbarung fristlos aus wichtigem Grund kündigen, wenn der Auftraggeber schwerwiegend gegen seine Pflichten verstößt.

Ein wesentlicher Verstoß gegen diese Vereinbarung ist auch ein wesentlicher Verstoß gegen den Hauptvertrag.

5.3 Hekatron haftet gegenüber dem Auftraggeber für Schäden, die Hekatron, ein von ihr mit der Verarbeitung betrauter Mitarbeiter oder ein Unterauftragnehmer bei der Erbringung der vertraglichen Leistung schuldhaft verursacht. Für Schäden, die ein Betroffener wegen unzulässiger oder unrichtiger Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, kommt der Auftraggeber gegenüber den Betroffenen auf. Soweit der Auftraggeber dabei zu Schadensersatz verpflichtet ist, bleibt ihm der Rückgriff auf Hekatron vorbehalten.

5.4 Sollte das Eigentum des Auftraggebers bei Hekatron oder seinen Unterauftragnehmern durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so verständigt Hekatron den Auftraggeber unverzüglich.

Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Anlage 1

Technische und organisatorische Maßnahmen

Hekatron setzt auf Experten, die mit geeigneten Maßnahmen zur Qualität, Robustheit und Datensicherheit des Systems Genius Plus beitragen. Dieses Dokument fasst die Maßnahmen von Hekatron als **Anbieter**, diva-e als Entwickler und **Betreiber** und Securiton AG (Secure-Online-Platform / SOP) als **Provider** zusammen.

Das System Genius Plus als Ganzes wird als **System** bezeichnet. Eine Softwarekomponente des Systems wird als **Dienst** bezeichnet. Eine Maschine, auf dem ein Dienst des Systems läuft, wird als **Server** bezeichnet. Alle erfassten oder eingegebenen Daten (Liegenschaft, Ansprechpartner, Melderstatus, ...) werden als **Kundendaten** bezeichnet.

1 Zutrittskontrolle

Ziel: Nur Berechtigte erhalten Zutritt zu den Datenverarbeitungsanlagen.

Bei Anbieter, Betreiber und Provider erfolgt der Zutritt mithilfe eines elektronischen **Schließsystems**. Für den Fall, dass das elektronische Schließsystem ausfällt, sind Schlüssel an dokumentierte Personen ausgegeben. Besucher werden stets von einem Mitarbeiter begleitet.

Auf dem **Mobilgerät** des Nutzers werden alle Kundendaten gespeichert. Dies gilt sowohl für die mit dem Gerät erfassten Daten als auch für Daten aus der Genius Cloud, die auf das Gerät synchronisiert werden. Die physische Sicherheit des Mobilgeräts liegt ausschließlich in Nutzerhand.

Die Kundendaten aller Nutzer werden im **Rechenzentrum** zusammengeführt. Zum Rechenzentrum haben nur die Mitarbeiter des Providers Zutritt. Der Zutritt zum Rechenzentrum wird protokolliert und mithilfe einer Videoaufzeichnung und Gegensprechanlage überwacht.

Der Zutritt zu den **Büroräumen** des Providers ist mit denselben Maßnahmen gesichert. Die Büroräume des Betreibers sind in den oberen Etagen eines Hochhauses und sind nur über eine Etagentür erreichbar.

2 Zugangskontrolle

Ziel: Nur Berechtigte können die Datenverarbeitungsanlagen nutzen.

Nutzer erlangen über Genius Web im Browser oder über die auf ihrem Mobilgerät installierte Genius Pro App Zugang zum System Genius Plus. Die **Anmeldung** erfolgt mit E-Mail-Adresse und Passwort. Das Passwort wird

mit einem geeigneten Verfahren gespeichert. Hekatron, Betreiber und Provider haben über die Anmeldung keinen Zugang zu Kundendaten.

Im Browser bleibt ein Nutzer so lange an Genius Web angemeldet, bis er sich **abmeldet** oder das Browser-Fenster schließt. In der App bleibt er so lange angemeldet, bis er sich abmeldet oder in Genius Web abgemeldet wird. Bis dahin fragt die App das Passwort bei einem Neustart nicht ab.

Der **Zugang zu Diensten** erfolgt nur über verschlüsselte Verbindungen. Nur vom Konfigurationsserver des Betreibers aus sind die Dienste beim Provider erreichbar. Zugang zum Konfigurationsserver haben nur Administratoren des Betreibers, deren Schlüssel hinterlegt wurden. Es sind nur Schlüssel der Administratoren hinterlegt, die das System warten.

Die Administration der Dienste erfolgt in den Büroräumen des Betreibers. Um bei Störungen auch außerhalb der Bürozeiten reagieren zu können, haben einige Mitarbeiter einen Fernzugang zum Netzwerk des Betreibers. Die Anmeldung an diesem **Fernzugang** erfolgt mit Benutzer-Zertifikaten.

Nur zur Inbetriebnahme und zur Störungsbeseitigung an den Servern kann der Provider **Zugang zum Server** (Konsole) erlangen. Zur Störungsbehebung außerhalb der Bürozeiten hat er eine Rufbereitschaft.

Der Provider betreibt die Sicherheits- und Angriffserkennungssysteme des Rechenzentrums selbst. Der Betreiber hat keinen Zugriff auf diese Sicherheitssysteme. In der **Firewall** sind nur die zum Betrieb des Dienstes und zur Administration benötigten Adressen und Ports freigeschaltet, Produktiv- und Administrationsnetz sind getrennt.

Hekatron, Betreiber und Provider haben für ihre **interne Datenverarbeitung** Richtlinien für Sicherheit und Datenschutz festgelegt und Verantwortliche benannt. Sie unterweisen ihre Mitarbeiter und schützen ihre Datenverarbeitung durch Maßnahmen nach dem Stand der Technik, u.a. durch Benutzerverwaltung, Softwareverteilung, sichere Zugänge zum Firmennetzwerk und Verschlüsselung mobiler Datenträger.

3 Zugriffskontrolle

Ziel: Nur Berechtigte können Daten lesen, kopieren, verändern oder entfernen.

Auf **Mobilgeräten** werden Kundendaten mit den vom Mobilbetriebssystem zur Verfügung gestellten Funktionen verschlüsselt gespeichert. Dies verhindert den Datenzugriff durch andere auf dem Gerät installierte Apps. In der App kann der Nutzer auf alle darin gespeicherten Daten zugreifen.

Entfernt ein Nutzer auf einem Android-Gerät mit einer Version kleiner 6.0 die Gerätesperre, löscht Android den Schlüssel der App. Dies ist ein Fehler

in Android, durch den noch nicht synchronisierte Wartungsdaten gelöscht würden. Daher wird auf solchen Geräten **nicht verschlüsselt**.

Genius Cloud verwendet eine Programmbibliothek, die durchgängige Sicherheitsfunktionen bereitstellt. Alle Ein- und Ausgaben werden anhand hinterlegter Kriterien geprüft und ggf. abgewiesen. Der Zugriff auf die Datenbank erfolgt mittels vorbereiteter Abfragen über Objekte. Die Kombination dieser Maßnahmen gewährleistet, dass Nutzer nur auf die Kundendaten ihres Unternehmens zugreifen können.

4 Weitergabekontrolle

Ziel: Daten können bei der Übermittlung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Die Übermittlung ist nur an die vorgesehenen Stellen möglich.

Kundendaten werden nicht auf mobilen **Datenträgern** gespeichert. Alle Datenübertragungen innerhalb des Systems erfolgen über Netzwerkverbindungen. Abgesehen von Daten, die ein Nutzer an den Support schickt, werden Kundendaten nie an Stellen außerhalb des Systems übermittelt.

Die Datenübertragung zwischen Browser bzw. App und Genius Cloud ist **verschlüsselt**. Die App stellt nur dann eine Verbindung her, wenn sich die Genius Cloud mit einem in der App hinterlegten Zertifikat ausweist. Im Browser werden Angriffe auf die sichere Datenübertragung durch zusätzliche Protokolle verhindert oder erkannt.

Die Genius Cloud versendet **E-Mails** zur Einrichtung neuer Nutzer und zum Rücksetzen von Passwörtern. Bis zum Hekatron-Mailserver wird verschlüsselt übertragen. Ob bei der weiteren Übermittlung verschlüsselt werden kann, hängt vom empfangenden Mailserver ab.

5 Eingabekontrolle

Ziel: Es ist nachvollziehbar, wer Daten eingegeben, verändert oder gelöscht hat.

Um eine **eindeutige Zuordnung** der Nutzer zu gewährleisten, wird die E-Mail-Adresse eines Nutzers als sein Benutzername verwendet. Das System lässt die Einladung eines weiteren Nutzers nur zu, wenn seine E-Mail-Adresse noch nicht im System angelegt ist.

Die **Anmeldung am Server** ist mit einem auf dem Konfigurationsserver hinterlegten Schlüssel möglich. Durch die Anmeldung am Konfigurationsserver ist nachvollziehbar, wer den Serverschlüssel benutzt hat.

Protokolliert werden alle Anmeldungen, Aktionen in der Nutzerverwaltung und die Kommandos zur Konfiguration auf dem Konfigurationsserver. Nicht protokolliert wird, welcher Nutzer welche Daten ändert.

Zur **Fehlersuche** kann die Protokollierung für einzelne Transaktionen eingeschaltet werden. Hierbei werden Daten allenfalls pseudonymisiert gespeichert.

Nutzer haben keinen **Zugriff auf Protokolle**. Administratoren werten die Protokolle mithilfe von Werkzeugen aus.

6 Auftragskontrolle

Ziel: Daten werden nur entsprechend den Auftragsvorgaben verarbeitet.

Die gemeinsame **Entwicklung** des Systems erfolgt nach den Prinzipien der agilen Softwareentwicklung. Eine robuste Architektur, der Einsatz bewährter Softwarekomponenten, umfangreiche Testroutinen und regelmäßige interne Code-Reviews führen zu guter Codequalität, welche durch unabhängige Penetrationstests bestätigt wird.

Sicherheit und Datenschutz werden bei der Entwicklung berücksichtigt (Security / Privacy by Design). Hekatron und der Betreiber überprüfen regelmäßig Technik und Prozesse – beim Betrieb und bei der Weiterentwicklung. Gefundene Mängel werden unverzüglich beseitigt.

Nutzer verarbeiten ihre Daten selbst. Nur zur **Fehlerbehebung** wird der Betreiber Kundendaten direkt bearbeiten. Die betroffenen Nutzer prüfen selbst, ob die Daten nach der Korrektur sachlich korrekt sind.

7 Verfügbarkeitskontrolle

Ziel: Daten sind gegen zufällige Zerstörung oder Verlust geschützt.

Das **Mobilgerät** kann verloren gehen, entwendet oder zerstört werden. Es kann von Hekatron nicht geschützt werden. Daher weist Hekatron den Nutzer regelmäßig auf die Vorteile der Anbindung an die Genius Cloud hin: Dann gehen nur die seit der letzten Synchronisation erfassten Daten verloren.

Damit Nutzer Daten nicht aus Versehen löschen, werden vor dem **Löschen größerer Datenmengen** deutliche Warnungen angezeigt. Nur Nut-zer mit administrativen Rechten können andere Nutzer löschen und Geräte sperren. Da hierbei auf dem Mobilgerät erfasste aber noch nicht synchronisierte Daten gelöscht werden, wird der Nutzer auch hier gewarnt.

Beim Betrieb der Dienste werden Inkonsistenzen durch automatisierte Konfiguration vermieden. Die Einstellung aller **Betriebsparameter** ist dokumentiert. Bei Fehlern nach Änderungen an der Konfiguration kann die vorherige Einstellung leicht wiederhergestellt werden.

Die je Dienst ergriffenen Maßnahmen unterscheiden sich nach Ausfallwahrscheinlichkeit und Bedeutung für das System. Alle Server haben unterbrechungsfreie Stromversorgung und werden überwacht. Einige Dienste sind gedoppelt, die meisten nutzen **redundante Speichersysteme** und eine redundante Netzwerkanbindung.

Kundendaten und Konfiguration werden regelmäßig gesichert (Backup). Von Kernsystemen wird zusätzlich eine Kopie erstellt (Image). Die **Datensicherungen** liegen in einem mehrere Kilometer entfernten Backup-Rechenzentrum des Providers. Der Betreiber testet regelmäßig, ob Systeme und Daten wiederherstellbar sind.

8 Trennungskontrolle

Ziel: Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet.

Die von den Nutzern im System erfassten Daten werden **nicht zu unterschiedlichen Zwecken** erhoben.

Da Hekatron keinen Zugriff auf Kundendaten hat, muss Hekatron den Betreiber beauftragen, Auswertungen zu programmieren (**4-Augen-Prinzip**). Der Auftrag muss vom Datenschutzbeauftragten freigegeben werden. Er achtet darauf, dass Auswertungen anonymisiert, pseudonymisiert oder hinreichend zusammengefasst sind, sodass kein Rückschluss auf einzelne Personen mehr möglich ist.

Die Entwicklung neuer Funktionalität erfolgt nicht im Produktivsystem, sondern in einer dafür aufgesetzten **Entwicklungsumgebung**. In der Entwicklungsumgebung wird nicht mit Echtdaten gearbeitet.