Vereinbarung zur Auftragsverarbeitung

zwischen

ISA Informations-, Schloss- und Alarmtechnik GmbH
Am Jägersberg 20
24161 Altenholz
Deutschland

im folgenden Auftragnehmer genannt

und

Firma: _____
Straße, Hausnummer: _____
Postleitzahl, Ort: _____
Land: _____

im folgenden Auftraggeber genannt.

Der Auftragnehmer und Auftraggeber sind gemeinsam die Parteien.

Grundlage der Vereinbarung

Die Parteien haben einen oder mehrere Verträge über die Erbringung von Leistungen durch den Auftragnehmer abgeschlossen, im Rahmen derer der Auftragnehmer gegebenenfalls personenbezogene Daten im Auftrag vom Auftraggeber verarbeitet (Auftragsverarbeitung).
Um diese Auftragsverarbeitung entsprechend den gesetzlichen Anforderungen vertraglich zu regeln, schließen die Parteien diese Vereinbarung zur Auftragsverarbeitung (AV-Vereinbarung), welche die bestehenden vertraglichen Vereinbarungen zum Datenschutz mit Wirkung zum 25.05.2018 ersetzt.

1. Datenschutz

1.1. Bindung an gesetzliche Vorschriften und Zweckbindung

Die Parteien sind verpflichtet, alle einschlägigen Vorschriften zum Schutz personenbezogener Daten zu beachten. Bei der Erbringung der vertragsgegenständlichen Leistungen stellt der Auftragnehmer insbesondere sicher, dass alle Vorschriften zum Datenschutz, die für Auftragsverarbeiter unmittelbar anwendbar sind, eingehalten werden.
Der Auftragnehmer wird personenbezogene Daten, die er im Zusammenhang mit diesem Vertrag vom Auftraggeber oder von Dritten erhält, für diese anfertigt oder die ihm sonst zugänglich sind oder werden, ausschließlich zur Erbringung der vertraglich geschuldeten Leistungen verwenden. Zu einer anderweitigen Nutzung dieser Daten, insbesondere für Zwecke seines eigenen Geschäftsbetriebes oder für Zwecke Dritter, ist er nicht berechtigt.
Herr dieser Daten bleibt allein der Auftraggeber oder ggf. der Dritte, in deren Auftrag der Auftraggeber die Daten durch den Auftragnehmer verarbeiten lässt. Weitergehende gesetzliche und vertragliche Vertraulichkeitsverpflichtungen bleiben unberührt.

1.2. Beschreibung der Auftragsverarbeitungstätigkeiten

Eine Beschreibung der vom Auftragnehmer zu erbringenden Auftragsverarbeitungstätigkeiten ist in **Anlage 1** enthalten.

1.3. Technische und organisatorische Maßnahmen

Der Auftragnehmer ist verpflichtet, angemessene technische und organisatorische Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten zu ergreifen, die ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist, mindestens jedoch die technischen und organisatorischen Maßnahmen in **Anlage 2**.

1.4. Verpflichtung auf das Datengeheimnis

Der Auftragnehmer ist verpflichtet seine Beschäftigten über die einschlägigen gesetzlichen und vertraglich vereinbarten Datenschutzvorschriften ausführlich zu unterrichten und sie auf deren Einhaltung und zur Geheimhaltung zu verpflichten. Den Beschäftigten ist dabei insbesondere zu untersagen, personenbezogene Daten entgegen der Weisungen vom Auftraggeber zu verarbeiten. Die Geheimhaltungsverpflichtung wirkt auch nach Beendigung dieser Vereinbarung, sowie dem Arbeitsverhältnis der Beschäftigten fort.

1.5. Unterauftragsverhältnisse

Zu einer Vergabe von Unteraufträgen ist der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung vom Auftraggeber berechtigt; dies gilt auch für den Einsatz eines mit dem Auftragnehmer im Sinne von §§ 15 ff. AktG verbundenen Unternehmens.
Bei der Vergabe von Unteraufträgen verpflichtet sich der Auftragnehmer:

1.5.1. den Unterauftrag schriftlich im Rahmen eines Vertrags zu erteilen, in dem sichergestellt wird, dass die zwischen dem Auftraggeber und Auftragnehmer in diesem Artikel vereinbarten Regelungsinhalte auch gegenüber dem Unterauftragnehmer gelten; dieser Vertrag muss insbesondere eine genaue Beschreibung der unterbeauftragten Leistungen und der durch den Subunternehmer ergriffenen technischen und organisatorischen Maßnahmen enthalten sowie das Recht vom Auftraggeber (als Drittbegünstige) vorsehen, Kontrollrechte direkt gegenüber dem Unterauftragnehmer auszuüben;

1.5.2. auf Verlangen vom Auftraggeber Einblick in die relevanten Vertragsunterlagen mit dem Unterauftragnehmer zu gewähren;

1.5.3. den Unterauftragnehmer regelmäßig und in angemessener Weise auf die Einhaltung der Vorgaben zu kontrollieren und die Ergebnisse der Kontrollen zu dokumentieren; und

1.5.4. in Abstimmung mit dem Auftraggeber sicherzustellen, dass bei dem Unterauftragnehmer ein angemessenes Datenschutzniveau im Sinne des anwendbaren Datenschutzrechts gewährleistet wird (z.B. durch den Abschluss der Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern (2010/87/EU) zwischen dem Unterauftragnehmer und dem Auftraggeber und/oder den Dritten (Auftraggeber -Kunden).

1.6. Berichtigung, Löschung und Sperrung von Daten; Weisungsrechte und Mitwirkungspflichten des Auftragnehmers

Über die Berichtigung, Löschung und Sperrung von Daten entscheidet allein der Auftraggeber.
Der Auftragnehmer wird Weisungen vom Auftraggeber, die sich auf den Umgang mit den verarbeiteten personenbezogenen Daten beziehen, befolgen. Ist er der Ansicht, dass eine Weisung vom Auftraggeber rechtswidrig ist oder gegen die Bestimmungen dieses Vertrags verstößt, so ist er verpflichtet, den Auftraggeber hierauf unverzüglich hinzuweisen.
Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Einhaltung des für den Auftraggeber geltenden Datenschutzrechts zu unterstützen, insbesondere im Rahmen der Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber.

1.7. Beendigung des Auftrags

Im Falle der Beendigung des Auftrags hat der Auftragnehmer die ihm überlassenen oder im Rahmen der Auftragserarbeitung erstellten personenbezogenen Daten - vorbehaltlich anderer vertraglicher Vereinbarungen oder Vorgaben seitens des Auftraggebers - zurückzugeben und im Verfügungsbereich des Auftragnehmers verbleibende Daten unwiederbringlich zu löschen bzw. zu vernichten. Die Löschung bzw. Vernichtung ist dem Auftraggeber auf Verlangen schriftlich zu bestätigen.

1.8. Mitteilungspflichten

1.8.1. Der Auftragnehmer ist verpflichtet, dem Auftraggeber unverzüglich bei Eintritt oder bei begründetem Verdacht des Eintritts einer der im folgenden genannten Vorfälle zu informieren:
(i) Verstöße gegen diesen Artikel oder gegen gesetzliche Datenschutzbestimmungen, einschließlich Fälle des Zugriffs oder Verlusts, der Nutzung, Zerstörung, Löschung, Übermittlung, Weitergabe oder Offenlegung von personenbezogenen Daten, wenn diese rechtswidrig und/oder weder durch den Auftraggeber noch durch diesen Vertrag ausdrücklich erlaubt ist, in keinem Bezug zur Leistungserbringung unter diesem Vertrag steht und/oder einer Meldepflicht nach geltendem Recht unterliegt oder
(ii) sonstige Unregelmäßigkeiten, Störungen oder Vorfälle beim Umgang mit personenbezogenen Daten, die im Auftrag vom Auftraggeber verarbeitet werden.

1.8.2. Der Auftragnehmer verpflichtet sich auf eigene Kosten
(i) im Benehmen mit dem Auftraggeber die Vorfälle umfassend aufzuklären,
(ii) entsprechende Abhilfemaßnahmen zu treffen und
iii) dem Auftraggeber bei der Erfüllung gegebenenfalls bestehender gesetzlicher Informationspflichten gegenüber betroffenen Personen oder Behörden zu unterstützen.

1.8.3. Der Auftragnehmer hat dem Auftraggeber folgendes mitzuteilen:
(i) den Zeitpunkt des Vorfalls
(ii) eine Beschreibung des Vorfalls,
(iii) die Namen der Personen, deren personenbezogene Daten möglicherweise betroffen sind sowie eine Beschreibung der Art der betroffenen personenbezogenen Daten.

1.8.4. Der Auftragnehmer verpflichtet sich, dem Auftraggeber unverzüglich, spätestens jedoch innerhalb von sieben Tagen, über
(i) Beschwerden oder Anfragen von betroffenen Personen (z.B. bezüglich der Berichtigung, Löschung oder Sperrung von Daten) oder
(ii) Anordnungen oder Anfragen von Aufsichtsbehörden oder Gerichten zu unterrichten und diesbezügliche Weisungen vom Auftraggeber einzuholen.

1.9. Kontrollrechte und Haftung

Der Auftraggeber ist berechtigt, ohne dass der Auftragnehmer in diesem Zusammenhang die Erstattung von Kosten verlangen kann, die Einhaltung der dem Auftragnehmer obliegenden Pflichten, insbesondere im Hinblick auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen, im jeweils erforderlichen Umfang selbst oder durch Dritte durch Kontrollmaßnahmen beim Auftragnehmer zu überprüfen oder nach seiner Wahl schriftliche Auskünfte, Bestätigungen und Unterlagen anzufordern. Der Auftragnehmer wird den Auftraggeber hierbei umfassend unterstützen, insbesondere durch die Begleitung von Kontrollmaßnahmen auch vor Ort, Abgabe von Eigenerklärungen oder Vorlage von Zertifikaten Dritter. Die vorstehenden Kontrollrechte stehen auch jeglichen Dritten unmittelbar zu, deren Daten vom Auftraggeber im Auftrag (und somit vom Auftragnehmer im Unterauftrag) verarbeitet werden.
Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner. Für die Haftung im Einzelnen gilt Art. 82 DSGVO). Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subunternehmer im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen. Eine Haftung des Auftragnehmers tritt nicht ein, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

2. Sonstiges

2.1. Diese AV-Vereinbarung endet automatisch mit Beendigung des Vertrags bzw. im Falle des Bestehens mehrerer Verträge, mit dem Ende des am längsten laufenden Vertrags. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

2.2. Im Falle von Widersprüchen zwischen den Bestimmungen dieser AV-Vereinbarung und den Bestimmungen eines bestehenden Vertrags gehen die Bestimmungen dieser AV-Vereinbarung in Bezug auf die datenschutzrechtlichen Rechte und Pflichten der Parteien vor. Besteht Unklarheit darüber, ob sich eine Bestimmung auf datenschutzrechtliche Rechte und Pflichten der Parteien bezieht, gilt im Zweifel diese AV-Vereinbarung.

2.3. Die Aufhebung, Nebenabreden, Änderungen und Ergänzungen dieser AV-Vereinbarung bedürfen der Schriftform. Auf dieses Formerfordernis kann nur schriftlich verzichtet werden.

2.4. Sollten einzelne Bestimmungen dieser AV-Vereinbarung ganz oder teilweise unwirksam sein oder unwirksam werden oder sich aus Rechtsgründen nicht in der beabsichtigten Weise vollziehen lassen, so ist hiervon die Wirksamkeit der AV-Vereinbarung im Übrigen nicht berührt. Die Parteien werden partnerschaftlich zusammenwirken, um eine Regelung zu finden, die der unwirksamen Bestimmung in ihrem ursprünglichen Maß so nahekommt, wie dies rechtlich möglich ist.

Auftraggeber:

_____
Ort, Datum

_____
Name (Druckbuchstaben)

_____
Unterschrift

Auftragnehmer:

_____
Ort, Datum

_____
Name (Druckbuchstaben)

_____
Unterschrift

Anlage 1 – Beschreibung der Auftragsverarbeitungstätigkeiten

Leistungsempfänger
Leistungsempfänger ist der Auftraggeber sowie dessen Kunden.

Auftragnehmer
Der Auftragnehmer erbringt Leistungen in Zusammenhang mit gebäudetechnischen Systemen (Installations-, Störungsbeseitigungs-, Inbetriebsetzungs-, Datensicherungs-, Wartungs-, Inspektions- und/oder Instandsetzungsleistungen) für den Auftraggeber und seine Kunden, vor Ort oder im Wege des Fernzugriffs.

Betroffene Personen
Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

- Mitarbeiter des Auftraggebers oder des Kunden des Auftraggebers und ggf. seiner Dienstleister/Kunden, die das jeweilige Produkt betreiben und/oder konfigurieren
- Besucher/unternehmensfremde Dritte, die den überwachten Bereich betreten

Kategorien von Daten
Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien:

- Personenstammdaten (Name, Benutzername, Personalnummer, Büroadresse, Gültigkeit der Zutrittsberechtigung etc.);
- Geschäftliche Kontaktdaten (E-Mail-Adresse, Telefonnummer);
- Zutrittsdaten (Ort und Zeitpunkt von Zutritten);
- IP-Adressen von Endgeräten mit denen auf das System zugegriffen wurde;
- geloggte Aktivität (z.B. Änderungen an der Konfiguration des Systems);
- nur bei Videoüberwachungsprodukten: Videoaufzeichnungen

Besondere Datenkategorien (falls zutreffend):
Die übermittelten personenbezogenen Daten umfassen folgende besondere Datenkategorien:

_____

_____

_____

Verarbeitung
Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:

- Installation/Inbetriebsetzung von gebäudetechnischen Systemen: Vom Auftraggeber oder seinen Kunden für die vertragsgegenständlichen Systeme zur Verfügung gestellte Personenstammdaten werden in den Systemen hinterlegt und den vom Auftraggeber oder seinen Kunden vorgegebenen Berechtigungen zugeordnet.
- Störungsbeseitigung an gebäudetechnischen Systemen (vor Ort oder im Wege des Fernzugriffs): In den vertragsgegenständlichen Systemen abgelegte Daten (z.B. Namen von Mitarbeitern, in Log-files protokollierte Nutzeraktionen) können eingesehen werden; im Falle von Systemen zur Video-Überwachung können die von den Kameras erstellten Aufnahmen erfasster Personen gesehen werden.
- Wartungs-, Inspektions- und Instandsetzungsleistungen (vor Ort oder im Wege des Fernzugriffs): In den betroffenen Systemen abgelegte personenbezogene Daten (z.B. Namen von Mitarbeitern, in Log-files protokollierte Nutzeraktionen) können eingesehen werden; im Falle von Systemen zur Video-Überwachung können die von den Kameras erstellten Aufnahmen erfasster Personen gesehen werden.
- Back-up-Services zu gebäudetechnischen Systemen (vor Ort oder im Wege des Fernzugriffs): Dateien mit personenbezogenen Daten des Kunden vom Auftraggeber (z.B. Benutzernamen im Anlagen-Log und deren Aktivitäten, Namen von Mitarbeitern und deren Zutritte zu bestimmten Sicherheitsbereichen oder Aufzeichnungen von Videoüberwachungssystemen) werden ausgelesen und auf Sicherungsmedien (z.B. Portable Drive, lokale Server) gespeichert und ggf. zurückgespielt.

Anlage 2 – Technische und organisatorische Maßnahmen

1. Einleitung

In diesem Dokument werden die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten (Maßnahmen) beschrieben, die der Auftragnehmer im Zusammenhang mit der von ihm durchgeführten Verarbeitung unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen mindestens trifft.

2. Grundlegende Maßnahmen

Die grundlegenden Maßnahmen gewährleisten den Schutz der Vertraulichkeit und der Integrität der Systeme, mit denen der Auftragnehmer personenbezogene Daten verarbeitet, insbesondere im Wege des Fernzugriffs. Diese Maßnahmen gelten für alle vom Auftragnehmer durchgeführten Verarbeitungen, sofern nicht im zugrundeliegenden Vertrag abweichend vereinbart.

2.1. Innerbetriebliche Organisation

Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt. Alle Mitarbeiter und Dienstleister des Auftragnehmers mit Zugriff auf personenbezogene Daten werden verpflichtet, diese nur auf Anweisung und ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen zu verarbeiten.

2.2. Schutz vor unbefugtem Zugang

Unbefugten ist der Zutritt zu Geschäftsräumen oder Rechenzentren, in denen Datenverarbeitungstätigkeiten stattfinden, zu verwehren.

Maßnahmen:

Der Auftragnehmer schützt die Gebäude oder Geschäftsräume durch angemessene Zutrittskontrollsysteme basierend auf einer Sicherheitseinstufung der Gebäude oder Geschäftsräume und entsprechend definiertem Zutrittsberechtigungskonzept. Alle Gebäude oder Geschäftsräume sind durch technische Zutrittskontrollmaßnahmen z.B. unter Verwendung einer elektronischen Schließanlage gesichert. Abhängig von der Sicherheitseinstufung werden Grundstücke, Gebäude oder einzelne Bereiche durch zusätzliche Maßnahmen gesichert. Dazu können spezielle Zutrittsprofile, Video-Überwachung und anderes gehören.
Zutrittsrechte für autorisierte Personen werden gemäß den festgelegten Kriterien individuell erteilt. Dies gilt auch hinsichtlich externer Personen.

2.3. Schutz von Rechnern

Die für die Verarbeitung verwendeten Rechner sind gegen unbefugte Nutzung abzusichern und zu schützen.

Maßnahmen:

Zugang zu Rechnern (z.B. Notebooks, Workstations) erhalten nur authentifizierte Benutzer unter Verwendung von bspw. folgenden Maßnahmen: Datenverschlüsselung, individualisierte Passwortvergabe (mind. 8 Zeichen, regelmäßig automatisch verfallend), automatische Systemsperrung bei Inaktivität. Der Schutz der verwendeten Rechner gegen Angriffe sowie gegen zufällige oder mutwillige Zerstörung oder Änderung erfolgt u.a. durch Intrusion Detection-Systeme, Firewalls und regelmäßig aktualisierte Malware-Filter.

2.4. Schutz von Daten bei der Weitergabe, beim Transport und beim Fernzugriff

Es ist dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Maßnahmen:

Absicherung der elektronischen Kommunikationswege durch Einrichtung geschlossener Netzwerke und Verfahren zur Datenverschlüsselung. Sofern ein physischer Datenträger-Transport erfolgt,

werden die Daten nur verschlüsselt transportiert. Fernwartungsverbindungen werden mittels Verschlüsselung geschützt. Datum, Art und Umfang der Fernwartung werden protokolliert.

3. Spezifische Maßnahmen für Leistungen, bei denen der Auftragnehmer Daten des Auftraggebers-Kunden bzw. sonstiger Dritter in IT-Systemen speichert

Diese spezifischen Maßnahmen gewährleisten den Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme, in denen der Auftragnehmer Daten des Auftraggeber-Kunden bzw. sonstiger Dritter speichert. Sie finden Anwendung, wenn die Speicherung von Daten maßgeblicher Bestandteil der vertragsgegenständlichen Leistungen des Auftragnehmers darstellt und nicht bloß vorübergehend erfolgt.

3.1. Schutz vor unbefugter Verarbeitung

Es ist zu gewährleisten, dass die zur Benutzung eines IT-Systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen:

Zugriff auf personenbezogene Daten in IT-Systemen wird auf der Grundlage eines rollenbezogenen Berechtigungskonzepts gewährt. Ferner werden bei Bedarf unberechtigte Zugriffe auf personenbezogene Daten durch Datenverschlüsselung verhindert.

3.2. Gewährleistung der Nachvollziehbarkeit

Es ist zu gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Der Auftragnehmer erlaubt nur authentifizierten Benutzern auf der Grundlage eines rollenbezogenen Berechtigungskonzepts den Zugriff auf personenbezogene Daten. Zugriffe auf personenbezogene Daten werden in Log-Dateien erfasst, die deren Erstellung, Veränderung und Entfernung detailliert protokollieren.