Vereinbarung über eine gemeinsame Verantwortlichkeit

zwischen

dem Vertragspartner der Anmietung einer Video Guard Videoüberwachungslösung

– Verantwortlicher (A) –

und der

International Security GmbH, Wehrden Ost 5, 26835 Hesel

– Verantwortlicher (B) oder ISG –

1. Gegenstand der Vereinbarung

(1) Zwischen den Parteien besteht ein Vertragsverhältnis, dass die gemeinsame Verarbeitung von Daten durch die Verantwortlichen (A) und (B) beinhaltet. Die Parteien sind sich darüber einig, dass sie im Hinblick auf dieses Zusammenwirken gemeinsam über Zwecke und Mittel der Verarbeitung i.S.d. Art. 4 Nr. 7 DSGVO bestimmen und insoweit eine gemeinsame Verantwortlichkeit besteht.
(2) Dieser Vertrag stellt die Vereinbarung zwischen gemeinsam Verantwortlichen i.S.d. Art. 26 DSGVO zwischen den Parteien dar. In diesem Vertrag werden Regelungen dazu getroffen, wer welchen Verpflichtungen der DSGVO im Zusammenhang mit gemeinsam Verarbeitung personenbezogener Daten nachkommt.

2. Beschreibung der Datenverarbeitung

(1) Zweck, Art und Umfang der Verarbeitung personenbezogener Daten ergeben sich aus dem zwischen den Parteien geschlossenen Hauptvertrag sowie der insoweit ggf. zusätzlich einbezogenen vertraglichen Regelungen.
(2) Die Art der Daten sowie die Kategorien betroffener Personen sind der Anlage 1 dieses Vertrages zu entnehmen.

3. Verantwortlichkeit und Zuständigkeiten für Verarbeitungsschritte/-phasen

(1) Die Parteien haben in der Anlage 2 dieses Vertrages die Verarbeitungsschritte, die der gemeinsamen Verantwortlichkeit unterliegen, beschrieben und die jeweiligen Verantwortlichkeiten zugewiesen. Wenn keine Angaben erfolgen und der Vertrag auch ansonsten keine Verantwortlichkeiten zuweist, ist davon auszugehen, dass die Parteien gleichermaßen für die Verarbeitung der jeweiligen Datenart(en) verantwortlich sind.
(2) In der Anlage 2 können die Parteien ferner Verantwortlichkeiten für die Bearbeitung und Umsetzung von Maßnahmen festlegen, die anlässlich der Wahrnehmung der Rechte von Betroffenen aus den

Art. 15-21 DSGVO zu treffen sind. Wenn keine Angaben erfolgen und der Vertrag auch ansonsten keine Verantwortlichkeiten zuweist, ist davon auszugehen, dass beide Parteien gleichermaßen für die Bearbeitung von vorgenannten Betroffenenanfragen verantwortlich sind.

(3) Ungeachtet der Regelungen in Absatz 1 und 2 stimmen die Parteien überein, dass sich betroffene Personen an beide Parteien zwecks Wahrnehmung der ihnen jeweils zustehenden Betroffenenrechte wenden können. In einem solchen Fall ist die jeweils andere Partei dazu verpflichtet, das Ersuchen eines Betroffenen an die nach Anlage 2 dieses Vertrages zuständige Partei unverzüglich weiterzuleiten. Die Parteien werden sich hierfür gegenseitig Kontaktadressen benennen und jede Änderung unverzüglich in Textform mitteilen.

4. Umsetzung von Betroffenenrechten

(1) Jede Partei ist verpflichtet, die Informationspflichten aus Art. 12-14 DSGVO und Art. 26 Abs. 2 S. 2 DSGVO gegenüber den Betroffenen umzusetzen, soweit die jeweilige Partei für den/die Verarbeitungschritt(e)/-phase(n) im Sinne der Ziff. 3 dieses Vertrages zuständig ist.

(2) Betroffenen Personen sind die erforderlichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache unentgeltlich zur Verfügung zu stellen.

(3) Die Parteien können in **Anlage 2** primäre Verantwortlichkeiten für die Erfüllung der Informationspflichten aus den Art. 12-14 DSGVO vereinbaren.

5. Datensicherheit

Die Parteien verpflichten sich gegenseitig zur Einhaltung der jeweils nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, soweit dies die Verarbeitung personenbezogener Daten betrifft, für die eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DSGVO besteht.
Eine generelle Übersicht über bestehende Mindestanforderungen bei technisch organisatorischen Maßnahmen ist in der **Anlage 3** einzusehen.

6. Meldepflichten bei Datenschutzverletzungen

(1) Jede Partei wird die jeweils andere Partei unverzüglich über jede Verletzung des Schutzes personenbezogener Daten i.S.d. Art. 4 Nr. 12 DSGVO in Textform unterrichten. Die Parteien werden sich gegenseitig unverzüglich alle Informationen im Zusammenhang mit der Datenschutzverletzung zur Verfügung stellen, die zur Prüfung der Datenschutzverletzung und seiner Folgen sowie für die Erfüllung etwaiger Meldepflichten nach den Art. 33, 34 DSGVO erforderlich sind.

(2) Für den Fall, dass eine Meldepflicht nach Art. 33 DSGVO besteht, werden die Parteien im Rahmen der Zumutbarkeit das weitere Vorgehen abstimmen und sich bei der Erfüllung der Meldepflichten gegenseitig unterstützen.

(3) (3) Sofern eine Benachrichtigung der Betroffenen nach Art. 34 DSGVO erforderlich ist, werden die Parteien im Rahmen der Zumutbarkeit zusammenwirken und eine gemeinsame Benachrichtigung der Betroffenen durchführen, soweit die Parteien dies für sinnvoll halten.

7. Gemeinsame Pflichten

Alle Parteien haben sich gegenseitig unverzüglich und vollständig zu informieren, wenn Fehler oder Unregelmäßigkeiten bei der Datenverarbeitung oder Verletzungen von Bestimmungen dieses Vertrags oder anwendbaren Datenschutzrechts (insbesondere der DSGVO) festgestellt werden.

Die datenschutzkonforme Beschilderung an allen Zufahrten zum Überwachungsbereich muss durch den Auftraggeber sichergestellt werden. Der Auftragnehmer wird ergänzende Beschilderungsmaßnahmen durchführen.

8. Auftragsverarbeiter

(1) Die Beauftragung von Auftragsverarbeitern i.S.d. Art. 4 Nr. 8 DSGVO durch eine Partei bedarf der vorherigen Zustimmung der jeweils anderen Partei in Textform.
(2) Die jeweils andere Partei kann vor Erteilung der Zustimmung die Vorlage des Auftragsverarbeitungsvertrages verlangen, der mit dem jeweiligen Auftragsverarbeiter geschlossen wurde, um die Einhaltung der Vorgaben des Art. 28 DSGVO zu überprüfen.
(3) Sofern die Verarbeitung von personenbezogenen Daten in einem Drittland erfolgt, wird der Auftraggeber gegenüber der jeweils anderen Partei dieses Vertrages das Vorliegen der Garantien für ein angemessenes Datenschutzniveau im Drittland darlegen.
(4) Für den Fall, dass ein bestehender Auftragsverarbeitungsvertrag mit einem Auftragsverarbeiter geändert wird, besteht eine Informationspflicht des Auftraggebers gegenüber der jeweils anderen Partei dieses Vertrages. Für den Fall, dass die Änderung des Auftragsverarbeitungsvertrages zu einer Verletzung der Vorgaben aus Art. 28 DSGVO führt, kann die jeweils andere Vertragspartei von dem Auftraggeber eine unverzügliche Nachbesserung des Vertrages verlangen, damit die Voraussetzungen von Art. 28 DSGVO eingehalten werden.

9. Zusammenarbeit mit Aufsichtsbehörden

(1) Jede Partei ist verpflichtet, die jeweils andere Partei unverzüglich zu informieren, wenn eine Datenschutzaufsichtsbehörde sich an sie wendet und dies eine Verarbeitung betrifft, die von diesem Vertrag umfasst ist.
(2) Die Parteien werden die Beantwortung von Anfragen von Aufsichtsbehörden zu der vertragsgegenständlichen Verarbeitung miteinander abstimmen, soweit dies rechtlich zulässig und/oder zumutbar ist.
(3) Die Parteien sind sich darüber einig, dass aufsichtsbehördlichen Maßnahmen grundsätzlich Folge zu leisten ist. Gleichwohl werden die Parteien sich darüber ins Benehmen setzen, ob und inwieweit Rechtsbehelfe gegen Anordnungen der Behörde eingelegt werden.

10. Haftung

(1) Die Parteien haften gegenüber betroffenen Personen nach den gesetzlichen Vorschriften.
(2) Die Parteien stellen einander im Innenverhältnis von jeglicher Haftung frei, wenn die haftungsauslösende Ursache im Rahmen der Verantwortlichkeit nach Ziff. 3 dieses Vertrages allein von einer Partei zu vertreten ist. Das gilt auch im Hinblick auf eine gegen eine Partei etwa verhängte Geldbuße wegen eines Verstoßes gegen Datenschutzvorschriften.

11. Schlussbestimmungen

(1) Für die Laufzeit und Beendigung des Vertrages gelten die Regelungen des Hauptvertrages. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.
(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem

Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 26 DSGVO am besten gerecht wird.

(3) Es gilt deutsches Recht einschließlich der DSGVO.

12. Einbeziehung in den Vermietungs- und Dienstleistungsvertrag

Das Dokument ist ohne Unterschrift gültig durch vertragliche Einbeziehung in den Vermietungs- und Dienstleistungsvertrag zwischen den Parteien.

Anlage 1

1. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Identifikationsdaten:
    - Name
    - Anschrift
    - Telefonnummer
    - Emailadresse
    - Beruf/Firma
    - Vertragsdaten
    - Kundennummer
- Abrechnungsdaten (des Auftraggebers):
    - Bankverbindung
    - Angebotsdaten
    - Kontakthistorie
- Sicherheitsdaten:
    - Videoüberwachung

2. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Besucher
- Externe Dienstleister
- Geschädigte
- Lieferanten
- Mitarbeiter des Auftraggebers

Generell: Personen im Aufzeichnungsbereich der Videoüberwachungsanlage

Anlage 2

VERARBEITUNGSTÄTIGKEIT	VERANTWORTLICHER	DATENKATEGORIEN
Video Guard (Normalbetrieb)	ISG	Video Alarme / gespeicherte Videoaufzeichnungen
Video Guard (Zugriff durch Auftraggeber)	ISG / Auftraggeber	Zugriff auf Livebilder / Angeforderte Aufzeichnungen
Videog Guard (im Schadensfall)	ISG / Auftraggeber	Zugriff auf Livebilder / Angeforderte Aufzeichnungen
Information von Betroffenen	ISG / Auftraggeber	Anfragen von Betroffenen / Weiterleitung an die ISG
Aufhängen von Beschilderungen	ISG / Auftraggeber	Auskünfte über Videoüberwa-chung

Anlage 3

Generelle Maßnahmen für Firma: International Security GmbH

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Einsatz einer Alarmanlage
    - Einsatz zum Schutz der Räumlichkeiten
- Bewegungsmelder
    - Innerhalb der Büroräume der International Security GmbH werden flächendeckend eingesetzt.
- Chipkarten-/Transponder-Schließsystem
    - Bereiche sind zusätzlich mit einem Transpondersystem gesichert.
- Manuelles Schließsystem mit Schließzylinder
    - Sicherheitsschließzylinder an allen Zugängen.
- Schlüsselregelung mit Dokumentation der Schlüssel (z.B. Schlüsselbuch)
    - Aus- und Rückgabe der Schließmedien wird dokumentiert. Ausgabe nur gegen Unterschrift der Beteiligten.

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort
    - Windowsdomäne mit eigenen Benutzernamen und Passwörtern.
- Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt)
    - Prozess zur Vergabe, Änderung und Entzug von Benutzerberechtigungen vorhanden. Zentrale Vergabe über die IT-Abteilung.
- Einsatz von Firewalls zum Schutz des Netzwerkes
    - Firewalls auf den eingesetzten Systemen aktiviert. Zugang zum Netzwerk zusätzlich geschützt.
- Sorgfältige Auswahl von Reinigungspersonal und Sicherheitspersonal

M.1.3 Beschreibung der Zugriffskontrolle:

- Erstellen und Einsatz eines Berechtigungskonzepts
    - Gruppenbasiertes Berechtigungsmanagement innerhalb der Windowsdomäne. Zugriffe auf Lotus Notes Datenbanken namensbasiert gesteuert.
- Einsatz von Aktenvernichtern
- Sichere Aufbewahrung von Datenträgern
    - Datenträger werden ausschließlich in der IT verwahrt. Zugang zu Datenträgern wird ausschließlich auf berechtigte Mitarbeiter minimiert.

M.1.4 Beschreibung der Weitergabekontrolle:

- Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung (softwareseitig)
    - Datentrennung durch Berechtigungen innerhalb der verwendeten Datenbanken
- Trennung von Produktiv- und Testsystem

M.1.6 Beschreibung der Pseudonymisierung:

- Trennung von Kundenstammdaten und Auftragsdaten

M.1.7 Beschreibung der Verschlüsselung:

- Verschlüsselte Datenübertragung (z.B., VPN, verschlüsselte Internetverbindungen mittels TLS/SSL)

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Einsatz von Antivirensoftware zum Schutz vor Malware
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- & Recovery Konzepts
- Feuer- und Rauchmeldeanlagen
- CO2 Feuerlöschgeräte in Serverräumen
- Erstellung und Anwendung von IT-Notfallplänen
- Klimaanlage in Serverräumen
- Redundante Datenhaltung (RAID 1 oder höher)
- Schutzsteckdosenleisten in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- (USV) Unterbrechungsfreie Stromversorgung

M.3.2 Beschreibung der Wiederherstellbarkeit:

- Regelmäßige und dokumentierte Datenwiederherstellungen
- IT-Notfallpläne und Wiederanlaufpläne

M.4 Weitere Maßnahmen

M.4.1 Beschreibung der Auftragskontrolle:

- Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

- Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- Benennung eines Datenschutzbeauftragten
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
- Verpflichtung auf die Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO

M.4.2 Beschreibung des Managementsystems:

- Durchführung regelmäßiger interner Audits
- Managementsystem zum Datenschutz (z.B. in Anlehnung an VdS 10010)
- Managementsystem zur Informationssicherheit (z.B. in Anlehnung an ISO 27001 oder VdS 3473)
- Durchführung regelmäßiger IT-Schwachstellenanalysen (z.B. Penetrationstest)
- Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)
- Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (audatis MANAGER)

Erhebungsbogen Technische und organisatorische Maßnahmen

Spezifische Maßnahmen für System Video Guard

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Manuelles Schließsystem mit Schließzylinder (Professional & Ultra)
    - Sicherheitsschließzylinder an der Außenhaut der eingesetzten Video Guard Systems. Schlüssel nur für das Wartungs- und Aufstellungspersonal verfügbar

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort
    - IT-System vor Ort (Netzwerkvideorekorder) wird mit Benutzername und Passwort geschützt. Passwortwechsel bei Weggang von Zugangsberechtigten.

M.1.3 Beschreibung der Zugriffskontrolle:

- Zugriffskontrolle auf lokalem System etabliert
    - Getrennte Benutzernamen und Passwörter für den Zugang auf die Aufzeichnungen.

M.1.4 Beschreibung der Weitergabekontrolle:

- Einrichtungen von VPN-Tunneln Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet
- Nutzung verschlüsselter Mobilfunkverbindungen
    - Einsatz mehrerer SIM-Karten zur Sicherstellung der Erreichbarkeit des Systems

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung (hardwareseitig)
    - Jeder Kunde erhält seine eigenen Systeme und Zugänge. Keine Vermischung von Kunden aufgrund der hardwareseitigen Trennung möglich.
- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
    - Speicherung der Daten getrennt nach Kunden
- Trennung von Produktiv- und Testsystem
    - Testsysteme werden getrennt von Produktivsystemen behandelt. Testsysteme werden im Rahmen von Wartungsarbeiten eingesetzt und dem Produktivbetrieb wieder zugeführt, wenn das Testsystem nicht mehr benötigt wird.

M.1.6 Beschreibung der Pseudonymisierung:

- Reine Daten zur Videoüberwachung sind nicht zu pseudonymisieren. Kundendaten werden soweit möglich über Kundennummern identifiziert

M.1.7 Beschreibung der Verschlüsselung:

- Verschlüsselte Datenspeicherung (u.a. Dateiverschlüsselung nach AES256 Standard)

    - Die Speicherung der Datenbestände erfolgt verschlüsselt auf eigenen Serversystemen und Netzwerkvideorekordern
- Verschlüsselte Datenübertragung (VPN, verschlüsselte Internetverbindungen mittels TLS/SSL)
    - Systeme sind mit mehreren SIM-Karten und einem VPN-Industrierouter ausgestattet.
    - Aufbau einer verschlüsselten VPN-Verbindung zu den Serversystemen der International Security GmbH.
    - Zugriff von Kunden nur über das VPN möglich.

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Nur einen technischen Administrationsaccount für Aufbau und technische Verwaltung

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Nur NVR-Technik.
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- (USV) Unterbrechungsfreie Stromversorgung
- Spannungskontrolle von außen auch für den Kunden sichtbar

M.3.2 Beschreibung der Wiederherstellbarkeit:

- Zwischenspeicherung auf den Serversystemen der International Security GmbH
    - Details sind den allgemeinen TOM zu entnehmen