Vereinbarung zur Auftragsverarbeitung

(gemäß EU-DSGVO Art. 28)

Zwischen

dem individuellen Mieter der Videoüberwachungslösung VIDEO GUARD

- im Folgenden: Auftraggeber –

und

Blömen VuS GmbH
Schuckertstraße 13, 48712 Gescher, Deutschland

- im Folgenden: Auftragsverarbeiter (nach Art. 28 EU-DSGVO) –

1. Allgemeine Bestimmungen und Auftragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 EU-DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind der **Anlage 1** zu entnehmen.

1.2 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 EU-DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 EU-DSGVO und die Wahrung der Betroffenenrechte verantwortlich.

1.3 Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der EU-DSGVO (Art. 44 - 50) und mit vorheriger Zustimmung des Auftraggebers.

1.4 Die Vergütung wird außerhalb dieses Vertrags vereinbart.

2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge zu leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

3.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.4 Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheits-gemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/-systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.

4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

4.3 Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragsverarbeiters

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2 Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 EU-DSGVO notwendigen technischen und organisatorischen Maßnahmen zu implementieren und das nach Art.

30 Abs. 2 EU-DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.

5.3 Sofern der Auftragsverarbeiter nach der EU-DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

5.4 Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice des Auftragsverarbeiters) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

5.5 Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b EU-DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

5.6 Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in **Anlage 2** dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 EU-DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.

6.2 Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen ständig und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

6.3 Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d EU-DSGVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

7. Unterstützungspflichten des Auftragsverarbeiters

7.1 Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e EUDSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 EU-DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

7.2 Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. ff EUDSGVO bei dessen Pflichten nach Art. 32 – 36 EU-DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1 Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer **(Siehe Anlage 1)**, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden.

8.2 Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit und Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragsverarbeiter wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

8.3 Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 EU-DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können. Der Auftragsverarbeiter ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragsverarbeiters einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.

8.4 Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. dem Subunternehmer zur Ausübung der gleichen Kontrollrechte wie ggü. dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.

8.5 Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und Art. 29 EUDSGVO ggü. den ihm unterstellten Personen erfüllt hat.

8.6 Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.

8.7 Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.

8.8 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 - 50 EU-DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragsverarbeiters

9.1 Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9.2 Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 EU-DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 EU-DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.

9.3 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

9.4 Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

11. Datengeheimnis und Vertraulichkeit

11.1 Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und die einschlägigen Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter bei Auftragserteilung auf die ggf. bestehenden besonderen Geheimnisschutzregeln hinzuweisen.

11.2 Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.

11.3 Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2 Sollte sich die EU-DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

- Anlagen -

Ort, Datum: Gescher, den

Unterschrift (Auftraggeber) Unterschrift (Auftragsverarbeiter)

Anlage 1 – Auftragsdetails

Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

Der Auftragsverarbeiter stellt dem Auftraggeber mobile Überwachungslösungen (VIDEO GUARD) zur Verfügung und betreibt diese. Diese mobilen Überwachungssysteme überwachen den Zutritt auf die privaten Gelände des Auftraggebers. Sollte es während der mit dem Auftraggeber vereinbarten Überwachungszeit, d.h. generell außerhalb der Arbeitszeiten, zu einem Alarm kommen, so verifiziert der Auftragsverarbeiter den Alarm und ergreift die vorher mit dem Auftraggeber abgestimmten Maßnahmen. Dem Auftraggeber kann je nach vorliegender Gefahr zuvor oder danach ein Videoclip des Alarms zur Verfügung gestellt werden. Die Videobilder werden in einem Ringspeicher gespeichert und nach individuell vereinbarter Speicherungsdauer automatisiert gelöscht bzw. überschrieben.

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

1. Identifikationsdaten: Name, Anschrift, Telefonnummer, Emailadresse, Beruf/Firma, Vertragsdaten, Kundennummer
2. Abrechnungsdaten: Bankverbindung, Angebotsdaten, Kontakthistorie
3. Sicherheitsdaten: Videoüberwachung

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

1. Insbesondere Mitarbeiter des Auftraggebers und von diesem mitgeteilte externe Ansprechpartner.
2. Insbesondere Firmendaten des Auftraggebers.
3. Alle Besucher des überwachten Bereichs (Videodaten).

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:

Der Zugriff der betroffenen Daten erfolgt über ein gesichertes Mobilfunknetz an ein DSGVO-konformes Rechenzentrum. Von dort über Festnetze an den Auftragsverarbeiter bzw. an seinen in der Anlage benannten Nachunternehmer.

Der Auftraggeber unterliegt folgenden besonderen Geheimnisschutzregeln, die auch vom Auftragsverarbeiter zu beachten sind:

1. § 203 StGB (Verletzung von Privatgeheimnissen)
2. § 204 StGB (Verwertung fremder Geheimnisse)
3. Art. 32 EU-DSGVO (Sicherheit der Verarbeitung u.a. Schutzziele nach Abs. 1)
4. Art. 33 EU-DSGVO (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde)
5. Art. 34 EU-DSGVO (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person)

Folgende Subunternehmer werden zur Auswertung der Videodaten und Einleitung der mit dem Auftraggeber vereinbarten Interventionen eingesetzt:

Alarmzentrale International Security GmbH, Wehrden Ost 5, 26835 Hesel, Deutschland

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen (TOM) des Auftragsverarbeiters nach Art. 32 EU-DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 EU-DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

I. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- ☑ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☑ Logische Mandantentrennung (softwareseitig)
- ☑ Berechtigungskonzept
- ☑ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☑ Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- ☑ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System
- ☑ Trennung von Produktiv- und Testsystem

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

1. Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

☑ End-to-End-Verschlüsselung bei der Weitergabe von Videodateien an den Auftraggeber

2. Pseudonymisierung

„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

☑ Ja, und zwar in folgender Art und Weise:

Kunden werden mit Kundennummern, Baustellen mit Projektnummern und Videodaten mit Kameranummern pseudonymisiert. Klare Trennung von Videodaten und personenbezogenen Daten.

3. Zutrittskontrolle

Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:

☑ Alarmanlage
☑ Absicherung von Gebäudeschächten
☑ Automatisches Zugangskontrollsystem
☑ Chipkarten-/Transponder-Schließsystem
☑ Manuelles Schließsystem
☑ Videoüberwachung der Zugänge
☑ Lichtschranken / Bewegungsmelder
☑ Sicherheitsschlösser
☑ Schlüsselregelung (Schlüsselausgabe etc.)
☑ Personenkontrolle beim Pförtner / Empfang
☑ Sorgfältige Auswahl von Reinigungspersonal
☑ Sorgfältige Auswahl von Wachpersonal
☑ Tragepflicht von Berechtigungsausweisen
☑ Zutrittskonzept / Besucherregelung

4. Zugangskontrolle

Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:

☑ Zuordnung von Benutzerrechten
☑ Erstellen von Benutzerprofilen
☑ Passwortvergabe
☑ Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
☑ Authentifikation mit biometrischen Verfahren
☑ Authentifikation mit Benutzername / Passwort
☑ Zuordnung von Benutzerprofilen zu IT-Systemen
☑ Gehäuseverriegelungen
☑ Einsatz von VPN-Technologie bei der Übertragung von Daten
☑ Verschlüsselung mobiler IT-Systeme
☑ Verschlüsselung mobiler Datenträger
☑ Verschlüsselung der Datensicherungssysteme
☑ Sperren externer Schnittstellen (USB etc.)
☑ Sicherheitsschlösser
☑ Schlüsselregelung (Schlüsselausgabe etc.)
☑ Personenkontrolle beim Pförtner / Empfang
☑ Sorgfältige Auswahl von Reinigungspersonal
☑ Sorgfältige Auswahl von Wachpersonal
☑ Tragepflicht von Berechtigungsausweisen
☑ Einsatz von Intrusion-Detection-Systemen
☑ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
☑ Einsatz von Anti-Viren-Software
☑ Verschlüsselung von Datenträgern in Laptops / Notebooks
☑ Einsatz einer Hardware-Firewall
☑ Einsatz einer Software-Firewall

5. Zugriffskontrolle

Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems 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:

- ☑ Berechtigungskonzept
- ☑ Verwaltung der Rechte durch Systemadministrator
- ☑ regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. Bei Ausscheiden von Mitarbeitern o.Ä.)
- ☑ Anzahl der Administratoren ist auf das „Notwendigste“ reduziert
- ☑ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☑ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☑ Sichere Aufbewahrung von Datenträgern
- ☑ physische Löschung von Datenträgern vor Wiederverwendung
- ☑ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☑ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☑ Protokollierung der Vernichtung
- ☑ Verschlüsselung von Datenträgern

6. Eingabekontrolle

Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- ☑ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☑ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☑ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☑ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

7. Auftragskontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- ☑ Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☑ vorherige Prüfung der und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- ☑ schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)
- ☑ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
- ☑ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt
- ☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☑ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- ☑ laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten
- ☑ Vertragsstrafen bei Verstößen

8. Transport- bzw. Weitergabekontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:

- ☑ Einsatz von VPN-Tunneln
- ☑ Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E-Mail-Verkehrs)
- ☑ Verschlüsselung physischer Datenträger bei Transport
- ☑ Einsatz einer datenschutzkonformen und verschlüsselten Betriebs-Cloud in Kooperation mit einem zertifizierten Rechenzentrum in Deutschland

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- ☑ Unterbrechungsfreie Stromversorgung (USV)
- ☑ Klimatisierung der Serverräume
- ☑ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☑ Schutzsteckdosenleisten in Serverräumen
- ☑ Feuer- und Rauchmeldeanlagen in Serverräumen
- ☑ Feuerlöschgeräte in Serverräumen
- ☑ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☑ Erstellen eines Backup- & Recoverykonzepts
- ☑ Testen von Datenwiederherstellung
- ☑ Erstellen eines Notfallplans
- ☑ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☑ Serverräume nicht unter sanitären Anlagen
- ☑ In Hochwassergebieten: Serverräume über der Wassergrenze
- ☑ belastbares Datensicherungs- und Widerherstellungskonzept vorhanden

IV. Besondere Datenschutzmaßnahmen

Es liegen schriftlich vor:

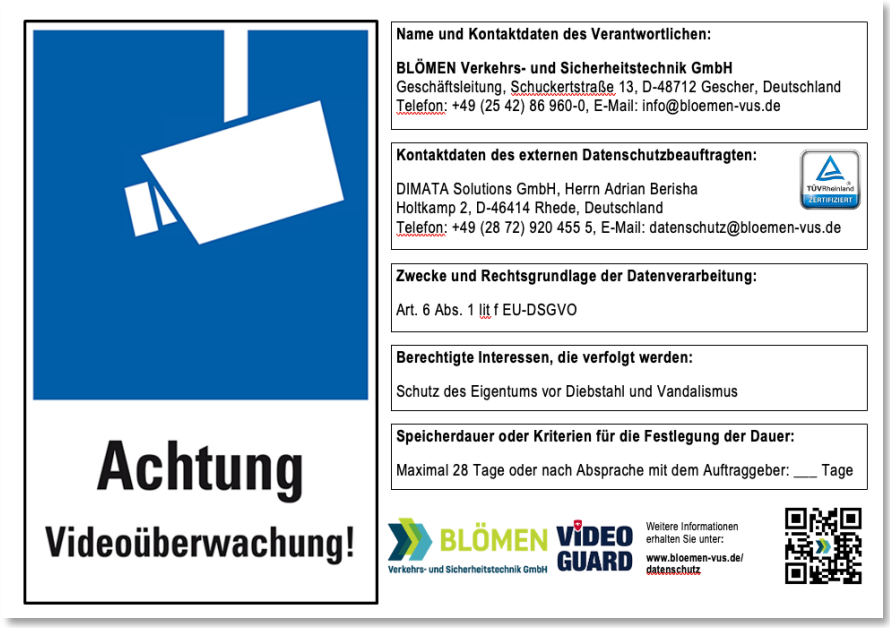
- ☑ interne Verhaltensregeln für Mitarbeiter (Datenschutz / Internet / E-Mail)
- ☑ Risikoanalyse
- ☑ Datenschutz-Folgenabschätzung
- ☑ Datensicherheitskonzept (intern / extern)
- ☑ Wiederanlaufkonzept
- ☑ Benennung eines externen Datenschutzbeauftragten (TÜV zertifiziert)
- ☑ Zertifikat: Prüfungsbericht IT-Sicherheitsprüfung liegen aktuell vor

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von 12 Monaten und anlassbezogen prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 - Hinweis zum Datenschutz Videoüberwachung

1. Wir informieren betroffene Personen mit unserem datenschutzkonformen Hinweisschild vor Betreten des zu überwachenden Bereichs.



Die maximale Speicherdauer der Videodaten beträgt 28 Tage oder nach Absprache mit dem Auftraggeber!

2. Die notwendigen Informationen auf dem Hinweisschild sind nach Art. 12 Abs. 7 EU-DSGVO in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form aufgeführt. Sie vermitteln einen datenschutzkonformen Überblick über die beabsichtigte Verarbeitung der Daten.

3. Mit einem gesonderten Hinweisblatt informieren wir über unsere Videoüberwachung auf der Grundlage des Art. 13 EU-DSGVO. Mit dieser Regelung sowie den sich aus Artikel 12 ff. EU-DSGVO ergebenden Anforderungen erfüllen wir unsere Transparenzpflichten gegenüber betroffenen Personen.

4. Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf die in Art. 15 EU-DSGVO im einzelnen aufgeführten Informationen.

5. Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender, unrichtiger personenbezogener Daten und ggf. die Vervollständigung unvollständiger personenbezogener Daten zu verlangen (Art. 16 EU-DSGVO).

6. Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 EU-DSGVO im einzelnen aufgeführten Gründe zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (Recht auf Löschung).

7. Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der in Art. 18 EU-DSGVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, für die Dauer der Prüfung durch den Verantwortlichen.

8. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen. Der Verantwortliche verarbeitet die personenbezogenen Daten dann nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 EU-DSGVO).

9. Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die EU-DSGVO verstößt (Art. 77 EU-DSGVO). Die betroffene Person kann dieses Recht bei einer Aufsichtsbehörde in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes geltend machen.

10. In Nordrhein-Westfalen ist die zuständige Aufsichtsbehörde:

Landesbeauftragte für Datenschutz und Informationsfreiheit
Kavalleriestraße 2-4,
40213 Düsseldorf
Telefon: +49 (2 11) 384 24 – 0
E-Mail: info@ldi.nrw.de

Anlage 4 - Datenschutzbeauftragter

Derzeit ist als **externer Datenschutzbeauftragter** beim Auftragsverarbeiter bestellt:

Adrian Berisha
DIMATA Solutions GmbH
Holtkamp 2
46414 Rhede

02861 / 825 29 - 30
datenschutz@bloemen-vus.de

Externer Datenschutzbeauftragter (TÜV Rheinland)
Zertifikatsnummer: 2866175