AVV

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO
Zwischen der
Wiesbadener Wach- und Schließgesellschaft Müller & Co. GmbH
Luisenstraße 19
65185 Wiesbaden
– nachfolgend "Auftragnehmer" genannt –
und dem jeweiligen Vertragspartner, mit dem ein Hauptvertrag über Sicherheitsdienstleistungen geschlossen wurde und der im Sinne von Art. 4 Nr. 7 DSGVO als Verantwortlicher handelt,
– nachfolgend „Auftraggeber" –
wird nachfolgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Präambel

Der Auftragnehmer erbringt umfassende Dienstleistungen im Bereich des Wach- und Sicherheitsgewerbes. Dazu gehören insbesondere die Durchführung von Objektschutz- und Revierdiensten, Empfangs- und Servicetätigkeiten, sowie der Betrieb einer Notruf- und Serviceleitstelle mit ergänzenden Online-Portalen. Zu den bereitgestellten Portalen zählen insbesondere:

- Portal für Alarmauslösungen (https://wachundschliess.amwin.de),
- Portal für Vertragsverwaltung (https://portal.notrufexperten.de),
- Portal „Bereitstellung" für Bild- und Videomaterial (https://portal.notrufexperten.de/web/bereitstellung),
- Portal „Timescan" für Leistungs- und Tätigkeitsnachweise im Revier- und Objektschutz (https://wachundschliess.timescan.de).

Im Rahmen dieser Tätigkeiten verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Diese Vereinbarung konkretisiert die Pflichten der Parteien nach Art. 28 DSGVO und legt die Rechte und Pflichten im Umgang mit personenbezogenen Daten fest.
Ein Auftragsverarbeitungsvertrag ist nur erforderlich, wenn der Auftraggeber selbst Verantwortlicher im Sinne der DSGVO ist. Dies ist regelmäßig bei Unternehmen, Vereinen oder Organisationen der Fall. Privatpersonen, die die Leistungen des Auftragnehmers ausschließlich zu persönlichen oder familiären Zwecken im Rahmen des sogenannten Haushaltsprivilegs (Art. 2 Abs. 2 lit. c DSGVO) nutzen – etwa bei einer Videoüberwachung, die sich ausschließlich auf das eigene Grundstück beschränkt –, benötigen keinen gesonderten AV-Vertrag. Überschreitet die Nutzung jedoch den rein privaten Bereich (z. B. Erfassung öffentlicher Flächen, Nachbargrundstücke oder allgemein zugänglicher Bereiche), gilt der Auftraggeber als Verantwortlicher im Sinne der DSGVO und dieser AV-Vertrag findet Anwendung.
Der Vertrag zur Auftragsverarbeitung kann auch in elektronischer Form gemäß Art. 28 Abs. 9 DSGVO geschlossen werden. Eine handschriftliche Unterschrift oder die Übersendung eines unterzeichneten Exemplars ist nicht erforderlich. Der Vertrag gilt als wirksam abgeschlossen, sobald der Auftraggeber den Hauptvertrag geschlossen hat und die Voraussetzungen einer Auftragsverarbeitung vorliegen. Der AV-Vertrag wird damit automatisch Bestandteil des Vertragsverhältnisses; einer gesonderten Unterzeichnung bedarf es nicht.

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser

Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.
(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der „Verarbeitung" i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

(1) Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten im Zusammenhang mit folgenden Tätigkeiten:

- Aufschaltung und Bearbeitung von Alarmmeldungen,
- Alarm- und Interventionsdienstleistungen,
- Objektschutz- und Revierdienste einschließlich Kontrollfahrten, Rundgänge, Schließdienste und Dokumentation von Tätigkeiten,
- Kontrolldienste im Rahmen von Veranstaltungen, Messen und ähnlichen Anlässen
- Empfangs- und Servicedienstleistungen, insbesondere Zutrittskontrollen, Besuchermanagement, Empfang, Poststelle und Ausweisprüfungen,
- Bereitstellung und Betrieb der Kundenportale (Alarmportal, Vertragsverwaltung, Portal „Bereitstellung", Portal „Timescan"),
- Speicherung, Auswertung und Übermittlung von Alarm-, Video- und Zutrittsdaten,
- Protokollierung von Portalzugriffen, Nutzeraktionen sowie Tätigkeitsnachweisen,
- Kunden- und Vertragsverwaltung, Rechnungswesen und Abrechnung,
- Erstellung von Angeboten und sonstiger Auftragsabwicklung.

(2) Zweck der Verarbeitung ist die Erbringung der im Hauptvertrag vereinbarten Sicherheitsdienstleistungen, einschließlich Online-Funktionen über die Kundenportale.
(3) Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt.

3. Art der Daten

(1) Folgende Arten personenbezogener Daten sind regelmäßig Gegenstand der Verarbeitung:

- Personenstammdaten (Name, Adresse, Kontaktdaten),
- Kommunikationsdaten (Telefonnummern, E-Mail),
- Kundendaten (Objektdaten, Ansprechpartner, Kontaktketten),
- Vertrags- und Abrechnungsdaten, Zahlungsinformationen,
- Besucherdaten (Name, Firma, Ausweisnummer, Besuchszweck, Ankunfts- und Abgangszeit),
- Zutritts- und Zugangsdaten (z. B. Protokolle über Ein- und Austritte, Zugangsberechtigungen, Schließprotokolle),
- Benutzer- und Zugangsdaten für die Portale,
- Protokolldaten zu Revisionen, Kontrollfahrten, Revierdiensten und Portalzugriffen,
- Videobilder, Bildmaterial, Alarmereignisdaten,
- Tätigkeits- und Leistungsnachweise im Rahmen von Objektschutz- und Revierdiensten.

4. Kategorien betroffener Personen

Folgende Kategorien betroffener Personen sind regelmäßig Gegenstand der Verarbeitung:

- Kunden und Ansprechpartner des Auftraggebers,
- Beschäftigte des Auftraggebers,
- Beschäftigte des Auftragnehmers (soweit systembezogen oder in Tätigkeitsnachweisen erfasst),
- Lieferanten, Errichter und Partner des Auftraggebers,
- Besucher, Gäste, Lieferanten, externe Dienstleister und sonstige Dritte, die im Rahmen von Zutrittskontrollen, Empfangs- oder Videoüberwachung erfasst werden.

5. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.
(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.
(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.
(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.
(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.
(8) Der Auftraggeber trägt die Verantwortung für die Richtigkeit und Aktualität der in den Portalen erfassten Stammdaten.
(10) Revisionen von Anlagen dürfen nur von autorisierten Errichtern oder Mitarbeitern veranlasst werden; die Verantwortung für die Zulässigkeit liegt beim Auftraggeber.

6. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.
(2) Der Auftragnehmer verarbeitet personenbezogene Daten, auch durch Unterauftragnehmer, ausschließlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (EWR). Eine Verarbeitung in einem Drittstaat außerhalb der EU/des EWR ist nur zulässig, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere:

- wenn ein Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO vorliegt, oder
- wenn geeignete Garantien nach Art. 46 DSGVO vereinbart wurden (z. B. EU-Standardvertragsklauseln, verbindliche interne Datenschutzvorschriften oder genehmigte Verhaltensregeln).

Der Auftragnehmer stellt in solchen Fällen sicher, dass die Rechte der betroffenen Personen gewahrt bleiben und weist dem Auftraggeber auf Verlangen die entsprechenden Nachweise und Vereinbarungen vor.
(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.
(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß

gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.
(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.
(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.
(7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.
(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.
(10) Der Auftragnehmer dokumentiert Zugriffe, Revisionen und Bearbeitungsschritte in den Portalen zur Nachvollziehbarkeit.

7. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Als Datenschutzbeauftragter ist beim Auftragnehmer:
Marcus Neuhaus, Luisenstraße 19, 65185 Wiesbaden, datenschutz@wachundschliess.de

8. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.
(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.
(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

9. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12–23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.
(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32–36 DSGVO genannten Pflichten.

10. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.
(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.
(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.
(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.
(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten, die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

11. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 1 zu diesem Vertrag angeben.
(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.
(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.
(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.
(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.
(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogene Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

12. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.
(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.
(3) Die Verpflichtung der Beschäftigten nach Absatz 2 ist dem Auftraggeber auf Anfrage nachzuweisen.

13. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12–23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.
(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.
(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit der Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

14. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Informationen Dritten zugänglich zu machen.
(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

15. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

16. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.
(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 2 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.
(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

17. Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen.
(2) Er ist mit einer Frist von drei Monaten zum Jahresende kündbar.
(3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

18. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.
(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.
(3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den

Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

19. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

20. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.
(2) Für Nebenabreden ist die Textform erforderlich. Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform. Dies gilt auch für die Änderung des Textformerfordernisses selbst.
(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage 1: Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten ("Unterauftragnehmer"). Dabei handelt es sich um folgende Unternehmen:

Unterauftragnehmer	Anschrift	Leistung	
Sadowsky KG	Neugasse 15–19, 65183 Wiesbaden, Deutschland	Server-Wartung	
INSOCAM GmbH	Nußbergstraße 11, 66119 Saarbrücken, Deutschland	Softwareanbieter für Alarmportal (AM/Win)	
Microsoft Corporation	One Microsoft Way, Redmond, WA 98052-6399, USA	Plattformanbieter (z. B. Microsoft Bookings)	
Cloudflare, Inc	101 Townsend Street, San Francisco, CA 94107-1934, USA	IT-Sicherheitsdienstleister / CDN & DDoS-Schutz	
SoftClean GmbH	Kanalstraße 28 23970 Wismar, Deutschland	Betrieb des Portals „Timescan": Erfassung, Verarbeitung und Bereitstellung von Leistungsnachweisen im Revier- und Objektschutz (Zeit-/Ortsstempel, Tätigkeitsberichte, Kunden-Exports)	
Brevo (Sendinblue GmbH)	Köpenicker Straße 126, 10179 Berlin, Deutschland	E-Mail-Marketing und Newsletter-Versand; Speicherung und Verwaltung von Kundenkontaktdaten (Name, E-Mail-Adresse, Statistiken zum Versand und Öffnungsverhalten)	Verarbeitung innerhalb der EU (Deutschland/Frankreich). Brevo nutzt ggf. Subdienstleister außerhalb der EU (z. B. CDN, Cloudanbieter). Für diese Fälle bestehen Standardvertragsklauseln (SCC) nach Art. 46 DSGVO. Details siehe: https://www.brevo.com/de/legal/privacypolicy/

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers
Der Auftragnehmer trifft folgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO:

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle:

- Die Server befinden sich in einem verschlossenen Serverraum innerhalb der Notruf- und Serviceleitstelle, zu dem nur ausgewählte Mitarbeiter Zutritt erhalten. Die Leitstelle ist ein gesondert gesicherter und bewachter Bereich, der nur über die Verwaltungsräume der Wiesbadener Wach- und Schließgesellschaft betreten werden kann.

- Die Notruf- und Serviceleitstelle ist rund um die Uhr mit Personal besetzt. Fenster und Türen sind besonders gesichert. Die Leitstelle ist zusätzlich durch Überfallmelder und Totmannschalter abgesichert. Eigene Alarme werden an eine externe Notruf- und Serviceleitstelle übertragen.

- Besucher der Notruf- und Serviceleitstelle müssen sich vorher anmelden und werden im Besucherbuch mit Namen, Datum und Zeit protokolliert.

- Nicht-Mitarbeiter dürfen die Leitstelle nur in Begleitung eines Mitarbeiters betreten.

- Die Verwaltungsräume der Wiesbadener Wach- und Schließgesellschaft sind durch eine Alarmanlage mit Bewegungsmeldern, Innensirene und Anbindung an die Notruf- und Serviceleitstelle geschützt. Die Eingänge sind videoüberwacht. Türen und Fenster der Verwaltungsräume sind außerhalb der Geschäftszeiten verschlossen. Nur Mitarbeiter haben Schlüssel zu den Firmenräumen; die Ausgabe und Rückgabe von Schlüsseln werden mit Unterschrift protokolliert.

- Notebooks werden außerhalb der Firmenräume durch verschlüsselte Festplatten, Anti-Viren-Programme und IPsec-Verbindungen geschützt.

Zugangskontrolle:

- Die Einrichtung und Änderung von Benutzerkonten erfolgt nach einem definierten Prozess. Bei Austritt eines Mitarbeiters werden alle zugehörigen Benutzerkonten gesperrt.

- Programm-Benutzerkonten sind grundsätzlich einer Person zuzuordnen. Windows-Benutzerkonten sind Gruppen oder Personen zuzuordnen.

- Standard-Benutzer haben keine Administratorrechte. Administratorrechte müssen über ein gesondertes Passwort freigeschaltet werden, das nur Administratoren kennen.

- Zur Vergabe von Passwörtern existieren klare Richtlinien:
    - Es dürfen keine Default-Passwörter verwendet werden.
    - Passwörter müssen hinreichend komplex sein (mindestens acht Zeichen, alphanumerisch und mindestens ein Sonderzeichen).
    - Passwörter dürfen nicht weitergegeben oder gemeinsam genutzt werden.
    - Geschäftliche Passwörter dürfen nicht privat verwendet werden.
    - Die Eingabe von Passwörtern muss unbeobachtet erfolgen.

- Der Zugriff auf Daten ist nur mit Passwort über das lokale Netzwerk oder über eine verschlüsselte Verbindung möglich.

- Programm-Passwörter müssen aus mindestens acht Zeichen bestehen und mindestens eine Zahl und ein Sonderzeichen enthalten.

Zugriffskontrolle:

- Berechtigungen für IT-Systeme und Applikationen werden ausschließlich von Administratoren eingerichtet.
- Berechtigungen werden grundsätzlich nach dem Need-to-know-Prinzip vergeben. Es erhalten nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten oder Systeme administrieren bzw. warten. Voraussetzung ist eine entsprechende Beantragung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten.
- Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet.
- Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

Trennung:

- Alle für Kunden eingesetzten IT-Systeme sind mandantenfähig. Kunden haben keinerlei Zugriff auf die Netzinfrastruktur. Kunden werden im System durch eigene Kunden- oder Objekt-Identnummern voneinander getrennt. Die Bediener haben – im Rahmen ihrer Berechtigungen – Zugriff auf die jeweils zugeordneten Kunden- oder Objektdaten.
- Die Trennung der Daten von verschiedenen Kunden ist stets gewährleistet.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Eingabekontrolle:

- Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.
- Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten.
- Benutzeraccounts dürfen nicht mit anderen Personen geteilt oder gemeinsam genutzt werden.

Weitergabekontrolle:

- Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt wurde oder soweit es zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.
- Soweit möglich, werden Daten verschlüsselt an Empfänger übertragen.
- Die Nutzung von privaten Datenträgern ist den Beschäftigten im Zusammenhang mit Kundendaten untersagt.
- Mitarbeiter werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf einen vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

Transportkontrolle:

- Die Übermittlung personenbezogener Daten erfolgt ausschließlich verschlüsselt (z.B. durch sicheren Upload/Download).
- Datenträger werden gemäß den Vorgaben des Auftraggebers transportiert.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Es existieren Maßnahmen, um sicherzustellen, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden: Daten auf IT-Systemen werden mindestens täglich inkrementell und wöchentlich vollständig gesichert.
- Die Sicherungsmedien werden verschlüsselt an einem physisch getrennten Ort aufbewahrt.
- Das Einspielen von Backups wird regelmäßig getestet.
- Es existiert ein Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

- Es wird ein Datenschutz-Management geführt.
- Es existiert eine Leitlinie zu Datenschutz und Datensicherheit sowie Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.
- Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
- Es ist sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem Datenschutzbeauftragten gemeldet werden. Der Datenschutzbeauftragte wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird sichergestellt, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.
- Bei der Verarbeitung von Daten für eigene Zwecke wird – falls die Voraussetzungen des Art. 33 DSGVO vorliegen – eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden des Vorfalls erfolgen.

Auftragskontrolle:

- Der Vertrag enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Der Vertrag enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Auftragnehmer außerhalb des schriftlich formulierten Auftrags.
- Mitarbeiter werden kontinuierlich auf die existierenden Richtlinien zur Einhaltung der technischen und organisatorischen Maßnahmen hingewiesen.