

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

- Auftrag -

Wird von Protection One ausgefüllt

475855	FUN-00200396	5068831
Kunden-Nr. / Debitor	Equipmentnummer	Angebot-Nr.

zwischen
Protection One GmbH - A Securitas Company
Rheinpromenade 10 · 40789 Monheim am Rhein
Telefon 02132-99 6 99-0 ·

im Folgenden: Auftragsverarbeiter und

Name/Firma:	Bürgerbad Kirchhoven gGmbH		
Straße:	Schwimmbadstraße 59/61	Ort: Heinsberg	PLZ: 52525
Standort:	Schwimmbadstraße 59/61, 52525 Heinsberg		

im Folgenden: Verantwortlicher

PRÄAMBEL

Dieser Vertrag zur Auftragsverarbeitung richtet sich nach der Verordnung (EU) 2016/ 679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/ 46/ EG (Datenschutz-Grundverordnung (DS-GVO)).

Dieser Vertrag bezieht sich auf den Fernüberwachungsvertrag zum Angebot **5068831**, nachstehend Hauptvertrag genannt, zwischen den Parteien.

Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten im Auftrag des Verantwortlichen nach Art. 28 DS-GVO (nachfolgend Auftrag genannt).

Die Vorschriften zur Auftragsverarbeitung kommen entsprechend zur Anwendung, wenn durch die Pflege oder Wartung einer Datenverarbeitungsanlage ein Zugriff der Beschäftigten des Auftragsverarbeiters auf personenbezogene Daten nicht ausgeschlossen werden kann.

Daraus resultierend wird Art. 28 DS-GVO analog angewendet, welcher die Rahmenbedingungen für die Verarbeitung von Daten im Auftrag beschreibt.

Dieser Vertrag findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte oder Beauftragte des Auftragsverarbeiters mit personenbezogenen Daten des Verantwortlichen in Berührung kommen oder kommen könnten.

INHALTSVERZEICHNIS

- § 1 Gegenstand und Dauer des Auftrages
- § 2 Konkretisierung des Auftragsinhalts
- § 3 Technisch-organisatorische Maßnahmen (TOM)
- § 4 Berichtigung, Einschränkung und Löschung von Daten, Auskunftserteilung
- § 5 Kontrollen und sonstige Pflichten des Auftragsverarbeiters
- § 6 Unterauftragsverhältnisse / Subunternehmer
- § 7 Rechte und Pflichten des Verantwortlichen, Duldungs- und Mitwirkungspflichten des Auftragsverarbeiters
- § 8 Mitteilungen bei Verstößen des Auftragsverarbeiters
- § 9 Weisungsbefugnis des Verantwortlichen
- § 10 Haftung
- § 11 Löschung von Daten und Rückgabe von Datenträgern
- § 12 Zuständige Datenschutz-Aufsichtsbehörde
- § 13 Informationspflichten, Schriftformklausel
- § 14 Schlussbestimmungen

Anlagen

- Anlage 1 - Technische Dokumentation bzw. Installationsvorgabe
- Anlage 2 - Begrifflichkeiten
- Anlage 3 - Beschreibung der Daten/Datenkategorien
- Anlage 4 - Beschreibung der Betroffenen/Betroffenengruppen
- Anlage 5 - Weisungsberechtigte Personen
- Anlage 6 - Genehmigte Subunternehmer und Nebendienstleister
- Anlage 7 - Technisch-organisatorische Maßnahmen des Auftragnehmers (TOM)
 - Anlage 7.1 - Zertifikat 1: Dienstleister für Sicherheitsanlagen nach DIN EN 16763
 - Anlage 7.2 - Zertifikat 2: VdS 3138 Notruf- und Serviceleitstelle
 - siehe auch VdS 2311 - Einbruchmeldeanlagen, Planung und Einbau
 - siehe auch VdS 2366 - Videoüberwachungsanlagen, Planung und Einbau
 - Anlage 7.3 - Zertifikat 3: VdS 10010 Datenschutz-Managementsystems
 - Anlage 7.4 - Zertifikat 4: VdS 10000 Informationssicherheits-Managementsystems

§ 1 GEGENSTAND UND DAUER DES AUFTRAGS

- (1) Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag. Gegenstand der Datenverarbeitung sind sämtliche personenbezogenen Daten vom Verantwortlichen, die der Auftragsverarbeiter im Rahmen der Erfüllung des Hauptvertrages verarbeitet oder auf die er Zugriff nimmt oder nehmen kann.
- (2) Für die Objekt- und Beweismittelsicherung zeichnet der Auftragsverarbeiter im Alarmfall Daten gem. dem Hauptvertrag auf und wertet diese aus. Zu diesem Zweck hat der Auftragsverarbeiter Sicherungseinrichtungen in den Räumlichkeiten des Auftraggebers installiert. Diese werden von einer zertifizierten Notruf- und Serviceleitstelle (siehe Anlage 7.2) überwacht, protokolliert und gesteuert.
- (3) Die genauen technischen Spezifikationen gehen aus dem Hauptvertrag und der technischen Dokumentation der kundenspezifischen Installationsvorgabe (siehe Hauptvertrag Anlage 1.1) hervor. Der Auftragsverarbeiter greift grundsätzlich nicht auf die Videoaufnahmen zu. Dies erfolgt nur im Alarmfall oder zu Wartungs- und Servicearbeiten, die auch im Rahmen einer Fernwartung stattfinden können. Der Auftragsverarbeiter nutzt die Daten zur Bearbeitung und Aufklärung eines Ereignisses (z.B. Alarm, Störung, Schadensfall), der durch seine Sicherungseinrichtungen bzw. durch Betätigen des Alarmknopfes durch den Verantwortlichen ausgelöst wurde. Video- und Audiodaten werden nur im Alarmfall automatisiert an den Auftragsverarbeiter übermittelt. Zugriffe zum Zweck von Fernwartungs- oder Servicearbeiten werden protokolliert. Die Aufzeichnungsgeräte beim Verantwortlichen verfügen, programmier- und geräteabhängig, über eine Ringspeicherung, deren Dauer vom Verantwortlichen festgelegt werden kann (siehe Anlage 1). Für den Betrieb der in den Räumlichkeiten des Verantwortlichen installierten Alarmzentrale sind personenbezogene Daten wie z. B. Namen von berechtigten Personen mit deren Rechten erforderlich. Außerdem fallen durch den Betrieb Nutzerdaten wie z. B. Benutzerkennung und Uhrzeit einer Scharf- oder Unscharfschaltung an. Grundsätzlich müssen im Alarmfall übermittelte Daten beim Auftragsverarbeiter 1 Jahr gem. der Euro-Norm für europäische Alarmempfangsstellen (DIN EN 50518) gespeichert werden, da dies zur Sachbearbeitung und Abwicklung des Auftrags im Interesse der Vertragsparteien erforderlich ist. Zugriff auf diese Daten haben nur die Mitarbeiter der Notruf- und Serviceleitstelle. In der Notruf- und Serviceleitstelle werden ein- wie ausgehende Telefongespräche, welche im Zuge einer Ereignisbearbeitung geführt werden, für 1 Jahr aus Gründen der Dokumentations- und Nachweispflicht gespeichert. Alle relevanten Daten aus Echtalarmen (Bedienertätigkeiten, Bilddateien, Tonaufnahmen) werden zur erweiterten Speicherung für zusätzlich 3 Jahre zwecks Dokumentation und Beweissicherung im Falle von Schadensersatzansprüchen gegenüber Protection One vorgehalten. Die gesetzliche Grundlage hierzu ist unser berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO i. V. m. § 195 BGB. Mit Ablauf der standardisierten Speicherdauer von 1 Jahr gem. DIN-EN 50518 tritt die erweiterte Speicherdauer in Kraft. Hiermit werden die Datenbündel in einen separaten, abgesicherten Datenspeicher überführt und lagern dort bis zum Ablauf der erweiterten Speicherdauer. Schlussendlich werden die Daten nach Wegfall der Rechtsgrundlage und der einhergehenden üblichen Karenzzeit zum Start des Folgejahres DSGVO-konform gelöscht.
- (4) Im Zuge einer Alarmbearbeitung werden ggf. (jedoch nicht ohne triftigen Grund) die vom Kunden hinterlegten Kontaktdaten an die Einsatzkräfte (Polizei) vor Ort weitergegeben, um alle notwendigen Schritte einleiten zu können.
- (5) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben. Die Geheimhaltungspflicht gilt darüber hinaus unbegrenzt.

§ 2 KONKRETISIERUNG DES AUFTRAGSINHALTS

- (1) Die Art der verwendeten personenbezogenen Daten, die Kategorie betroffener Personen, sowie Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen sind in dem Hauptvertrag und im § 1 dieses Auftragsverarbeitungsvertrags konkret beschrieben. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke als die der Vertragserfüllung. Bei den Wartungsaufgaben handelt sich um keine direkte Auftragsverarbeitung. Jedoch kann bei der Leistungserbringung eine Kenntnisnahme von personenbezogenen Daten nicht ausgeschlossen werden. Er darf von den ihm eingeräumten Zugriffsrechten nur in dem Umfang Gebrauch machen, der für die Durchführung der Wartungsarbeiten und vertraglich festgelegter Dienstleistung erforderlich ist.
- (2) Die Verarbeitung der Daten findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder in der Schweiz statt. Jede Verlagerung in ein sonstiges Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 3 TECHNISCH-ORGANISATORISCHE MASSNAHMEN (TOM)

- (1) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung (Art. 5 DS-GVO). Er wird in seinem Verantwortungsbereich die inner- betriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (siehe Anlage 7).
- (2) Der Auftragsverarbeiter setzt die technischen und organisatorischen Maßnahmen so um, dass die Verarbeitung im Einklang mit der DS-GVO erfolgt. Er hat dies zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben. Für den Fall, dass der Auftragsverarbeiter die Wartung und Pflege automatisierter Verfahren oder von Datenverarbeitungsanlagen im Wege der Fernwartung, also außerhalb der Geschäftsräume des Verantwortlichen, durchführt, hat der Auftragsverarbeiter die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Die Maßnahmen werden in Anlage 7 festgelegt. Soweit die Prüfung / ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen, sofern dem keine betrieblichen oder wirtschaftlichen Erfordernisse des Auftragsverarbeiters entgegenstehen. Wenn die Einhaltung der gesetzlichen Datenschutzvorschriften dem Grunde nach bereits gewährleistet war, erstattet der Verantwortliche dem Auftragsverarbeiter die durch die Umsetzung entstehenden Kosten.
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen und organisatorischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.
- (4) Der Auftragsverarbeiter hat die Sicherheit der Verarbeitung gem. Art. 28 Abs. 3 S.2 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO zu gewährleisten. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um die Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Einzelheiten in Anlage 7).

§ 4 BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN, AUSKUNFTSERTEILUNG

- (1) Der Auftragsverarbeiter hat personenbezogene Daten zu deren Berichtigung, Einschränkung und Löschung sowie zur Auskunftserteilung nur zu verarbeiten, wenn der Verantwortliche dies in dem Hauptvertrag oder in einer dokumentierten Weisung verlangt.
- (2) Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen an den Verantwortlichen unverzüglich weiterleiten.
- (3) Ist der Verantwortliche aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Verarbeitung von Daten zu erteilen, wird der Auftragsverarbeiter den Verantwortlichen dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Verantwortliche den Auftragsverarbeiter hierzu schriftlich oder in Textform aufgefordert hat und dem Auftragsverarbeiter die durch diese Unterstützung entstehenden Kosten erstattet, wenn diese über die Vorgaben der gesetzlichen Bestimmungen hinaus gehen. Der Auftragsverarbeiter wird ohne vorherige schriftliche Zustimmung des Verantwortlichen keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Verantwortlichen verweisen.

§ 5 KONTROLLEN UND SONSTIGE PFLICHTEN DES AUFTRAGSVERARBEITERS

- (1) Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er versichert, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften, insbesondere der DS-GVO, bekannt sind. Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.
- (2) Der Auftragsverarbeiter ist nicht berechtigt, die Daten an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (3) Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gem. Art. 28 ff. DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
- (4) Schriftliche Bestellung eines Datenschutzbeauftragten gem. Art. 37 DS-GVO, der seine Tätigkeit gem. Art. 38 f. DS-GVO ausübt. Aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers,
<https://www.protectionone.de/datenschutz>,
leicht zugänglich hinterlegt.
- (5) Der Auftragsverarbeiter gewährleistet die Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b DS-GVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die schriftlich auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
- (6) Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten gem. Art. 28 Abs. 3 S. 2 lit. a DS-GVO ausschließlich entsprechend der dokumentierten Weisung des Verantwortlichen verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Die Verpflichtung auf die Vertraulichkeit besteht auch nach Beendigung des Auftrags fort.
- (7) Sofern der Auftragsverarbeiter im Zusammenhang mit den Leistungen für den Verantwortlichen an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran Beteiligten schriftlich auf das (1) Fernmeldegeheimnis i.S.d. §3 TDDDG zu verpflichten.
- (8) Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.
- (9) Der Auftragsverarbeiter ist zur Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen verpflichtet.

Dabei kann der Nachweis auch durch die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-GVO, Vorlage eines Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Datenschutzbeauftragter) oder einer geeigneten Zertifizierung nach einem datenschutzspezifischen Zertifizierungsverfahren, sowie durch Datenschutzsiegel gem. Art. 42 DS-GVO, durch IT-Sicherheits- oder Datenschutzaudit (z.B. BSI-Grundschutz oder ISO 27001) erbracht werden.
- (10) Der Auftragsverarbeiter hat personenbezogene Daten nur zu verarbeiten, wenn der Verantwortliche dies in dem Hauptvertrag oder in einer dokumentierten Weisung verlangt (siehe § 4 (1)).

§ 6 UNTERAUFTRAGSVERHÄLTNISSE / SUBUNTERNEHMER

- (1) Der Verantwortliche ist damit einverstanden, dass der Auftragsverarbeiter zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragsverarbeiters zur Leistungserfüllung als Subunternehmer heranzieht und eine vertragliche Vereinbarung nach Maßgabe des Art 28 Abs. 2-4 DS-GVO zugrunde gelegt wird. Eine darüber hinausgehende Auslagerung auf Subunternehmer oder der Wechsel der Subunternehmer sind zulässig, soweit der Auftragsverarbeiter eine solche Auslagerung auf Subunternehmer dem Verantwortlichen mindestens 10 Tage vorab schriftlich oder in Textform anzeigt und der Verantwortliche nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen das geplante Unterauftragsverhältnis erhebt.
- (2) Der Auftragsverarbeiter wird den Subunternehmer nach dessen Eignung unter besonderer Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählen und einen Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO abschließen. Eine etwaige Prüfung durch den Verantwortlichen beim Subunternehmer erfolgt nur in Abstimmung mit dem Auftragsverarbeiter.
- (3) Als Unterauftragsverhältnisse sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht als Subunternehmerverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Post- und Versanddienstleistungen, externe Personaldienstleistungen, Reinigungskräfte, Wartung und Benutzerservice, ausschließliches Housing in einem externen Rechenzentrum, die Entsorgung von Datenträgern, Prüfer. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
- (4) Derzeit werden die in Anlage 6 genannten Subunternehmer eingesetzt.

§ 7 RECHTE UND PFLICHTEN DES VERANTWORTLICHEN, DULDUNGS- UND MITWIRKUNGSPFLICHTEN DES AUFTRAGSVERARBEITERS

- (1) Nach Art. 28 Abs. 1 DS-GVO ist der Verantwortliche dazu verpflichtet, nur mit Auftragsverarbeitern zusammenzuarbeiten, welche hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden. Der Verantwortliche verpflichtet sich zur Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere zur rechtmäßigen Datenweitergabe an den Auftragsverarbeiter.
- (2) Der Verantwortliche hat das Recht, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen vor Beginn der Datenverarbeitung beim Auftragsverarbeiter und sodann regelmäßig in angemessenem Umfang, im Benehmen mit dem Auftragsverarbeiter zu prüfen oder durch im Einzelfall zu benennende und zur Berufsschwiegenheit verpflichtete Prüfer/ Dritte durchführen zu lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Auftragsverarbeiter ist berechtigt, dem Verantwortlichen etwaige durch die Kontrollen entstandene Kosten in Rechnung zu stellen, wenn diese über die Vorgaben der gesetzlichen Bestimmungen hinaus gehen. Der Umfang der Kontrollen und daraus evtl. entstehende Kosten, müssen vor der Durchführung der Kontrollen mit dem Auftragsverarbeiter abgestimmt werden.
- (3) Darunter fallen insbesondere die Einholung von Auskünften bei dem Auftragsverarbeiter und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme, sowie sonstige Kontrollen vor Ort. Der Verantwortliche hat das Recht, sich innerhalb der üblichen Geschäftszeiten für einen Werktag ohne Störung des Betriebsablaufs durch Stichprobenkontrollen, die in der Regel 10 Werktage vorher anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Der Auftragsverarbeiter verpflichtet sich zur Duldung und Mitwirkung bei der Kontrolle, insbesondere dem Verantwortlichen auf schriftliche Anforderung Auskünfte zu erteilen und Nachweise zur Verfügung zu stellen, die zur Durchführung der Kontrolle erforderlich sind. Darunter fallen z.B. ein Nachweis über die Umsetzung der technischen und organisatorischen Maßnahmen und ein Nachweis über die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-GVO, falls vorhanden.
- (4) Sofern der Auftragsverarbeiter die Wartung und/oder Pflege der Videoanlagen auch im Wege der Fernwartung durchführt, wird der Auftragsverarbeiter von den ihm eingeräumten Zugriffsrechten auf Datenverarbeitungsanlagen des Verantwortlichen nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, als dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.
- (5) Der Auftragsverarbeiter ermöglicht dem Verantwortlichen eine wirksame Kontrolle der Fernwartungsarbeiten. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die es dem Verantwortlichen ermöglicht, die vom Auftragsverarbeiter durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.
- (6) Der Verantwortliche informiert den Auftragsverarbeiter, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (7) Die Pflicht zur Führung des Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 DS-GVO obliegt dem Verantwortlichen und ggf. seinem Vertreter. Auf Anfrage stellt der Verantwortliche der Behörde das Verarbeitungsverzeichnis zur Verfügung (Art. 30 Abs. 4 DS-GVO).

§ 8 MITTEILUNGEN BEI VERSTÖßEN DES AUFTRAGSVERARBEITERS

- (1) Alle Verstöße des Auftragsverarbeiters, der bei ihm beschäftigten Personen und der ggf. für ihn tätigen Subunternehmer, einschließlich deren etwaiger Subunternehmer, gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen, sind dem Verantwortlichen unverzüglich mitzuteilen, sofern sie die Verarbeitung der Daten des Verantwortlichen betreffen.
- (2) Im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten hat der Auftragsverarbeiter ohne Ansehen der Verursachung den Verantwortlichen zu informieren. Der Auftragsverarbeiter hat sich mit dem Verantwortlichen abzusprechen und angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Verantwortlichen Pflichten nach Art. 32 - 36 DS-GVO treffen, hat der Auftragsverarbeiter ihn hierbei zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen zur Verfügung zu stellen.

§ 9 WEISUNGSBEFUGNIS DES VERANTWORTLICHEN

- (1) Der Umgang mit den Daten erfolgt im Rahmen des getroffenen Vertrages und nach Weisung des Verantwortlichen. Der Verantwortliche behält sich im Rahmen der in diesem Vertrag getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht vor.
- (2) Weisungen werden grundsätzlich schriftlich erteilt. Mündliche Weisungen wird der Verantwortliche unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.
- (3) Weisungsberechtigte Personen ergeben sich aus Anlage 5.
- (4) Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner schriftlich der Nachfolger bzw. Vertreter mitzuteilen.
- (5) Änderungen, Ergänzungen oder Ersetzungen von Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Der Auftragsverarbeiter ist berechtigt, diese Leistungserweiterung abzulehnen oder dem Verantwortlichen entsprechend den Regelungen im Vertrag, im Übrigen gemäß seinen zum Leistungszeitpunkt geltenden Preisen, in Rechnung zu stellen.
- (6) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird. Sollten von einer solchen Verzögerung zwischen den Parteien vereinbarte Service Level bzw. Fristen betroffen sein, so werden diese während der Verzögerung ausgesetzt. Im Falle der Bestätigung trägt der Verantwortliche die volle Verantwortung für die Rechtmäßigkeit der Weisung und stellt den Auftragsverarbeiter von allen Ansprüchen Dritter sowie etwaigen wegen der Ausführung dieser Weisung gegen ihn verhängten Bußgelder frei. Im Falle einer Änderung der ursprünglichen Weisung gelten Satz 1 und 2 entsprechend.
- (7) Alle erteilten Weisungen sind sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter zu dokumentieren.

§ 10 HAFTUNG

Auf Art. 82 der DSGVO wird verwiesen

§ 11 LÖSCHUNG VON DATEN UND RÜCKGABE VON DATENTRÄGERN

- (1) Falls im Hauptvertrag nichts anderes vereinbart ist, hat der Auftragsverarbeiter aufgrund einer separat abzurechnenden Einzelbeauftragung durch den Verantwortlichen sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach dessen vorheriger schriftlicher Weisung datenschutzgerecht zu vernichten. Die Löschung bzw. Vernichtung ist dem Verantwortlichen auf Verlangen mit Datumsangabe schriftlich zu bestätigen. Das Protokoll der Löschung ist dem Verantwortlichen auf Anforderung vorzulegen.
- (2) Der Auftragsverarbeiter ist berechtigt, Daten, die zur Vertragserfüllung nicht mehr erforderlich sind, spätestens mit Beendigung des Hauptvertrages zu löschen.
- (3) Daten und Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.
- (4) Es ist gewährleistet, dass zur Verarbeitung/Löschung bestimmte Datenträger während ihres Transportes gegen unberechtigte Einsichtnahme und Verlust geschützt sind.

§ 12 ZUSTÄNDIGE DATENSCHUTZ-AUFSICHTSBEHÖRDE

- (1) Zuständige Aufsichtsbehörde für den Verantwortlichen ist

- (2) Zuständige Aufsichtsbehörde für den Auftragsverarbeiter ist die

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-
Westfalen Postfach 20 04 44
40102 Düsseldorf

0211/38424-0
poststelle@ldi.nrw.de

- (3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.
- (4) Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde zusammen im Sinne des Art. 31 DS-GVO.

§ 13 INFORMATIONSPFLICHTEN, SCHRIFTFORMKLAUSEL

- (1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt
- (2) Es gelten ausschließlich diese Bedingungen; Nebenabreden, Änderungen oder Ergänzungen dieser Bedingungen bedürfen für Ihre Wirksamkeit der Schriftform. Dieses gilt auch für die Abbedingung der Schriftformklausel

§ 14 SCHLUSSBESTIMMUNGEN

- (1) Änderungen und Ergänzungen dieses Vertrages und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Form und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrages handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (2) Die Regelungen dieses Vertrages gehen den Regelungen des Hauptvertrages vor.
- (3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht. In diesem Fall ist die unwirksame Bestimmung durch eine Regelung zu ersetzen, die dem Gewollten am nächsten kommt.
- (4) Der Gerichtsstand für alle Streitigkeiten aus diesem Vertrag entspricht dem aus dem zugrundeliegenden Hauptvertrag.

Ort, Datum

Monheim am Rhein, 03.08.2026

Protection One GmbH - A Securitas Company
Rheinpromenade 10
40789 Monheim am Rhein
Telefon: 02132 99 6 99 - 0
Telefax: 02132 99 6 99 - 217
E-Mail: zentrale@protectionone.de

Unterschrift Verantwortlicher

Unterschrift Auftragsverarbeiter

ANLAGE 1 - TECHNISCHE DOKUMENTATION BZW. INSTALLATIONSVORGABE

Bitte bei Erhalt (Installation) zu den Unterlagen legen!

ANLAGE 2 - BEGRIFFLICHKEITEN

Die Zutrittskontrolle verhindert den unbefugten Zutritt zu den Firmenbereichen des Unternehmens und regelt den Schutz besonders sensibler Bereiche. Die Zugangskontrolle verhindert, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können.

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Trennungskontrolle: Das Trennungsgebot gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Bei der Pseudonymisierung werden personenbezogener Daten in einer Weise verarbeitet, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechen- de technischen und organisatorischen Maßnahmen unterliegen.

Die Weitergabekontrolle gewährleistet, 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.

Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs- systeme eingegeben, verändert oder entfernt worden sind.

Die Verfügbarkeitskontrolle gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, dazu gehören Maßnahmen zur Sicherung der Anlagen ebenso wie zur Sicherung der Daten.

Auftragskontrolle: Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Anlage 3 - Beschreibung der Daten/Datenkategorien

- Personenstammdaten
- Vertragsstammdaten
- Kommunikationsdaten
- Abrechnungsdaten
- Auskunftangaben
- Kundenhistorie
- _____
- _____

ANLAGE 4 - BESCHREIBUNG DER BETROFFENEN/BETROFFENENGRUPPEN

- Kunden
- Interessenten
- Lieferanten / Dienstleister
- Ansprechpartner
- _____
- _____

ANLAGE 5 - WEISUNGSBERECHTIGTE PERSONEN

Ansprechpartner des Verantwortlichen sind:

Fachliche Zuständigkeit:

Funktion:

Erreichbarkeit:

Datenschutzrechtliche Zuständigkeit:

Funktion:

Erreichbarkeit:

Ansprechpartner des Auftragsverarbeiters sind:

Fachliche Zuständigkeit:

Funktion:

Leiter Sales Backoffice oder seine Vertreter

Erreichbarkeit:

salesbackoffice@protectionone.de

Datenschutzrechtliche Zuständigkeit:

Funktion:

Datenschutzbeauftragter oder Datenschutzkoordinator

Erreichbarkeit:

datenschutz@protectionone.de

ANLAGE 6 - GENEHMIGTE SUBUNTERNEHMER UND NEBENDIENSTLEISTER:

SUBUNTERNEHMER:

Pro Control GmbH (100-prozentige Tochter der Protection One GmbH) Rheinpromenade 10, 40789 Monheim am Rhein

Zweck/Auftragsinhalt:

Der Subunternehmer erbringt für die Protection One GmbH weisungsgebundene Dienstleistungen. Dies ist insbesondere der Betrieb der Notruf- und Serviceleitstelle.

Ort der Datenverarbeitung: Meerbusch und Monheim am Rhein

Sofern Smart Video Protect SVP Bestandteil des Hauptvertrages ist:

Morphean SA-HQ

Rte du Château 112, 1763 Granges-Paccot

Schweiz

Zweck/Auftragsinhalt:

Je nach vereinbartem Service die Speicherung und Analyse von Videodaten beim Subunternehmer.

Ort der Datenverarbeitung: Frankfurt am Main

Sofern Smart Data Protect Bestandteil des Hauptvertrages ist:

Deutsche Telekom

GmbH

Landgrabenweg 151, 53227 Bonn

Zweck/Auftragsinhalt:

Speicherung personenbezogener Daten der Kontaktpersonen für Terminabsprachen und zur Bearbeitung von Störungsmeldungen beim Subunternehmer.

Ort der Datenverarbeitung: Bonn

Sofern Zutrittskontrolle Bestandteil des Hauptvertrages ist:

Vanderbilt International (SWE) AB

Englundavägen 7

SE-171 40 Solna

Schweden

Zweck/Auftragsinhalt:

Speicherung personenbezogener Daten im Zuge der Zutrittskontrolle (AAC Acre Access Control)

Ort der Datenverarbeitung: Dublin/Irland

Sofern Schlüsselverwaltung oder sonstige Sicherheitsdienstleistungen Bestandteil des Hauptvertrages sind:

Securitas Alert Services GmbH

Besselstr. 13

68219 Mannheim

Zweck/Auftragsinhalt:

Speicherung personenbezogener Daten der Kontaktpersonen für Auftragsannahme

Ort der Datenverarbeitung: Mannheim

NEBENDIENSTLEISTER:

REMONDIS Rhein-Wupper GmbH & Co.

KG Karl-Hohmann-Straße 15-17, 40599

Düsseldorf

Zweck/Auftragsinhalt: Akten- und Datenträgervernichtung

Ort der Datenverarbeitung: Deutschland

Anlage 7 - TECHNISCH-ORGANISATORISCHE MASSNAHMEN DES AUFTRAGNEHMER (TOM)

A. VERTRAULICHKEIT

1. Zutrittskontrolle

- Der Zutritt zu den einzelnen Bereichen des Firmengebäudes wird durch eine zentrale Schließanlage sowie ein Chipkarten-/Transponder-Schließsystem gesichert.
- Es ist ein zentraler Empfang eingerichtet, der den Zutritt von betriebsfremden Personen kontrolliert. Innerhalb des Firmenbereichs werden die Besucher geführt. Jeder Mitarbeiter ist für seine Besucher verantwortlich.
- Nebenausgänge, Fluchttüren und sonstige Notausgänge können von außen nicht geöffnet werden. Eine Videoüberwachung ist an allen Zugängen installiert. Zusätzlich ist eine elektronische Alarmanlage installiert.
- Server und andere sicherheitskritische IT-Komponenten sind in abgeschlossenen Räumen mit Zutrittsmöglichkeit nur für berechtigte Personen untergebracht.

2. Zugangskontrolle

- Der Zugang zu den Datenverarbeitungssystemen ist mit Benutzerkennung und einem sicheren Passwort geschützt.
- Serversysteme sind nur mit Passwort und über eine passwortgeschützte, verschlüsselte Verbindung durch Benutzer mit Administratorrechten nutzbar. Clientsysteme sind nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar. Eine serverseitige Passwortrichtlinie sorgt für die automatische Umsetzung der Passwortrichtlinie.
- Es ist ein verbindliches Verfahren zur Vergabe von Berechtigungen implementiert. Eine eindeutige Zuordnung von Benutzerkonten zu Benutzern ist gewährleistet.

3. Zugriffskontrolle

- In den Datenverarbeitungssystemen sind rollenbasierte Berechtigungsprofile hinterlegt, in denen die zugriffsberechtigten Personen festgelegt und ihre Rechte hinterlegt sind.
- Zur Verhinderung und Erkennung von Angriffen werden Hard- und Software-Firewalls eingesetzt.
- Zum Schutz von Daten auf mobilen Geräten wird eine zentrale Smartphone-Administrations-Software genutzt.

4. Trennungskontrolle

- Die Trennung der Datenverarbeitung erfolgt je nach Verfahren auf Betriebssystem- oder Anwendungsebene. Test- und Produktionsdaten sind ebenfalls voneinander getrennt.
- Die Trennung der Daten unterschiedlicher Auftraggeber/Projekte erfolgt durch eine Equipmentnummer und Kundennummer, die der jeweiligen Überwachungskomponente zugewiesen werden.

5. Pseudonymisierung

- Hierfür erfolgt eine Maskierung von personenbezogenen Daten.

B. INTEGRITÄT

1. Weitergabekontrolle

- Die personenbezogenen und sonstigen vertraulichen Daten sind auf unterschiedliche Weise gegen unbefugten Zugriff und gegen unbefugtes Kopieren geschützt.
- Für die datenschutzkonforme Vernichtung vertraulicher Unterlagen ist ein zertifiziertes externes Entsorgungsunternehmen (siehe Anlage 6) beauftragt.

2. Eingabekontrolle

- Der folgende Ablauf gilt nur für die Mitarbeiter der Pro Control GmbH (siehe Anlage 6), aber nicht für die gesamte Protection One Unternehmensgruppe.
- Die Alarmempfangssoftware ist revisionssicher und entspricht den hohen Anforderungen der EN50518 bezüglich Speicherung und Änderung von personenbezogenen Daten. Durch das Managementsystem wird sichergestellt, dass alle Veränderungen nachvollziehbar abgespeichert werden.
- Durch die Benutzerverwaltung ist geregelt, wer personenbezogene Daten verarbeiten darf. Die Änderung von Stammdaten erfolgt immer im 4-Augen-Prinzip.
- Alle Mitarbeiter werden auf das Datengeheimnis verpflichtet und regelmäßig zum Thema Datenschutz geschult.

C. VERFÜGBARKEIT UND BELASTBARKEIT

1. Verfügbarkeitskontrolle

- Zur Gewährleistung einer zeitgerechten Wiederherstellung der Verfügbarkeit sind dem Stand der Technik entsprechende Sicherungstechnologien ein- gerichtet.
- Es ist ein vollständiges Backup-Konzept mit täglicher Sicherung eingerichtet.
- Der Einsatz von aktuellen Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) ist sichergestellt.
- Für den störungsfreien und sicheren Betrieb werden Storage Systeme mit Redundanz (RAID) und unterbrechungsfreier Stromversorgung eingesetzt.

D. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

1. Auftragskontrolle

- Dieser Punkt wird durch die vertraglichen Vereinbarungen zwischen den Parteien und die entsprechenden Kontrollrechte des Auftraggebers gewährleistet.

2. Audit

- Es finden regelmäßige Audits zur Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen statt.

ANLAGE 7.1 - ZERTIFIKATE

[Zertifizierungen - Protection One GmbH](#)