vollmergruppe dienstleistung

security parking cleaning services

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen

Auftraggeber,

und der

Westdeutscher Wachdienst GmbH & Co. KG, Neckarstr. 22-24, 45478 Mülheim an der Ruhr (Auftragnehmer),
vertreten durch den Geschäftsführer Herrn Andreas Brink

wird nachfolgend beschriebener Vertrag geschlossen:

§ 1 Gegenstand und Dauer des Auftrags

1. Gegenstand

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der vom Auftraggeber beauftragten Sicherheitsdienstleistungen. Die Verarbeitung kann insbesondere in folgenden Fällen erfolgen:

Viedeoalarmaufschaltung
Gegenstand des Auftrags ist die Aufschaltung und Überwachung von Videoübertragungssystemen des Auftraggebers in einer Notruf- und Serviceleitstelle (NSL).
Dabei verarbeitet der Auftragnehmer im Auftrag des Auftraggebers Bilddaten aus den Videoüberwachungssystemen, um sicherheitsrelevante Ereignisse zu erkennen, zu prüfen und gemäß den vereinbarten Interventionsmaßnahmen zu bearbeiten.

Alarmaufschaltung
Gegenstand des Auftrags ist die Aufschaltung und Bearbeitung von Alarmmeldungen aus Gefahrenmeldeanlagen (z. B. Einbruch-, Brand- oder technischen Alarmanlagen) des Auftraggebers in der Notruf- und Serviceleitstelle.
Dabei verarbeitet der Auftragnehmer alarmbezogene Daten sowie ggf. hinterlegte Kontakt- und Interventionsdaten, um Alarme zu prüfen und vereinbarte Maßnahmen einzuleiten.

Objektbewachung
Gegenstand des Auftrags ist die Durchführung von Bewachungs- und Sicherheitsdienstleistungen an Objekten des Auftraggebers.
Soweit im Rahmen der Leistungserbringung ein Zugriff auf Systeme des Auftraggebers (z. B. Zutrittskontrollsysteme, Besuchermanagement oder Sicherheitssoftware) erfolgt, kann es zur Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers kommen.

2. Dauer

Der Auftrag orientiert sich an der vereinbarten Vertragslaufzeit und kann von beiden Parteien mit einer Frist von einem Monat jederzeit gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 2 Konkretisierung des Auftragsinhalts

Einzelheiten zu Art und Zweck der vorgesehenen Verarbeitung oder Nutzung sind unter Buchstabe A. der Anlage 1 zu dieser Vereinbarung aufgeführt.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau ist festgestellt durch einen Angemessenheitsbeschluss der Kommission [Art. 45 Abs. 3 DSGVO];

- Das Schutzniveau wird beim Auftragnehmer durch verbindliche interne Datenschutzvorschriften [Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO] sowie,
- durch die Einhaltung von Standarddatenschutzklauseln [Art. 46 Abs. 2 litt. c und DSGVO] oder
- durch die Geschäftsführung eingeführte und genehmigte Verhaltensregeln [Art 46 Abs. 2 lit. e i.V.m. 40 DSGVO] hergestellt

Die Art der personenbezogenen Daten sind unter Buchstabe B. der Anlage 1 aufgeführt. Der Kreis der Betroffenen ist unter den Buchstabe C. der Anlage 1 aufgeführt.

§ 3 Technisch-organisatorische Maßnahmen

1. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur 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 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 DSGVO zu berücksichtigen [Einzelheiten in Anlage 2].
3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate

Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1.Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

- Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Roland Schroeder, SystemDatenschutzConsulting, Rebenlaube 12, 45133 Essen bestellt.
- Die Kontaktdaten des aktuellen Datenschutzbeauftragten sind der Homepage www.vollmergruppe.de des Auftragnehmers zu entnehmen.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 2].
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages.

§ 6 Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post- / Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2. Der Auftragnehmer ist berechtigt, Unterauftragnehmer einzusetzen. Änderungen in Bezug auf eingesetzte Unterauftragnehmer sind dem Auftraggeber unverzüglich mitzuteilen. Eine aktuelle Liste der Unterauftragnehmer ist der Anlage 3 zu entnehmen.
3. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
5. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers [mind. Textform].

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 7 Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, erfolgen durch:
   - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
   - aktuelle Testate, Berichte oder Berichtsauszüge des Datenschutzbeauftragten
4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
   a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
   b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
   c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
   d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
   e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 9 Weisungsbefugnis des Auftraggebers

1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich [mind. Textform].
2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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.
2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlagen

Anlage 1

A. Zu § 2 Ergänzungen zu Art und Zweck der Datenverarbeitung

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der vom Auftraggeber beauftragten Sicherheitsdienstleistungen. Weitere Einzelheiten zu Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung sind:

Video- und Bildaufnahmen werden nur bei entsprechend aufgeschalteten Kamerasystemen nach vorheriger, vertraglicher Absprache generiert.

Es findet keine permanente, sondern eine bedarfsgesteuerte Observation, nach Auslösung der installierten Gefahrenmeldetechnik, statt. Die Auswertung der übertragenen Videosequenzen wird in der VdS-zertifizierten Notruf- und Service-Leitstelle des Auftragnehmers vorgenommen.

Die Videoaufnahmen werden im Regelfall 72 Stunden gespeichert, um dem Auftraggeber bei Schadensfällen, auch nach aufeinanderfolgenden Feiertagen und Wochenenden, eine nachvollziehbare Dokumentation zur Verfügung stellen zu können.

Nach Ablauf des jeweils vereinbarten Zeitfensters werden die Daten gelöscht bzw. überschrieben.

B. Zu § 2 Art der personenbezogenen Daten

(maßgebliche Datenarten sind angekreuzt)

☒	Adressdaten	☒	Kontaktdaten	☒	Vertragsdaten	☐	Bankverbindungsdaten
☐	Kontodaten	☐	Abrechnungsdaten	☒	Leistungsdaten	☐	Finanzdaten
☐	Angebotsdaten	☐	Transaktionsdaten	☒	Mitarbeiterdaten	☐	Qualifikationsdaten
☐	Gesundheitsdaten	☐	Gesprächshistorie	☐	Auskünfte	☐	Personalverwaltung
☒	Videoaufzeichnungen	☐		☐		☐	

C. Zu § 2 Kreis der Betroffenen

(maßgebliche Personengruppen sind angekreuzt)

☒	Mitarbeitende	☐	Ruheständler	☒	Auszubildende	☒	Frühere Mitarbeiter
☒	Praktikanten	☐	Bewerber	☐	Unterhaltsberechtigte	☐	Angehörige
☒	Kunden	☒	Interessenten	☒	Lieferanten/Dienstleister	☒	Berater
☐	Makler	☒	Vermittler	☒	Mieter	☒	Gesellschafter
☐	Geschädigte	☐	Zeugen	☐	Dozenten	☒	Kontaktpersonen
☐	Pressevertreter	☐	Kunden	☒	Sonstige: alle auf dem Objektgelände befindliche Personen		

Anlage 2 - Technische und organisatorische Maßnahmen (TOM)

Anforderungen	Erfüllt	Nicht erfüllt
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)		
• Zutrittskontrolle Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen; --- • Umgesetzt durch: - Raumzutrittskontrolle über elektronische Funkschlüssel - Videoüberwachung der Zugänge - Schlüsselregelung - Alarmanlage - Personenkontrolle am Empfang	☒	☐
• Zugangskontrolle Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern; --- • Umgesetzt durch: • Zuordnung von Benutzerrechten • Passwortvergabe • Authentifizierung mit Benutzername • Schlüsselregelung • Sperren von externen Schnittstellen • Einsatz von Intrusion-Detection-System • Einsatz von Antiviren-Software • Einsatz einer Firewall • Erstellen von Benutzerprofilen • Einsatz von VPN-Technologie • Sicherheitsschlösser • Personenkontrolle am Empfang	☒	☐
• Zugriffskontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen; --- • Umgesetzt durch: – Anzahl der Administratoren auf das „Notwendigste“ reduziert – Protokollierung von Zugriffen auf Anwendungen, insbesondere bei Eingabe, Änderung und Löschung von Daten	☒	☐

– Physische Löschung von Datenträgern vor Wiederverwendung – Verwaltung der Rechte durch Systemadministrator – Passwortrichtlinie inkl. Passwortlänge, – Sichere Aufbewahrung von Datenträgern – Ordnungsgemäße Vernichtung von Datenträgern – Protokollierung der Vernichtung		
• Trennungskontrolle Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing; --- • Umgesetzt durch: – Logisch getrennte Speicherung – Erstellung eines Berechtigungskonzeptes – Festlegung von Datenbankrechten – Logische Mandantentrennung (softwareseitig) – Trennung von Produktiv- und Testsystemen	☒	☐
• Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen; --- • Umgesetzt durch: (bitte Maßnahme nachfolgend aufführen) – ….	☐	☒
2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)		
• Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur; --- • Umgesetzt durch: (bitte Maßnahme nachfolgend aufführen) – Einrichtungen von Standleitungen bzw. VPN-Tunneln	☒	☐
• Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement; --- • Umgesetzt durch: – Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen	☒	☐

– Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes		
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)		
• Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; --- • Umgesetzt durch: (bitte Maßnahme nachfolgend aufführen) – Unterbrechungsfreie Stromversorung (USV) – Geräte zur Überwachung von Temperatur – Feuer- und Rauchmeldeanlagen – Testen von Datenwiederherstellung – Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort – Klimaanlage in Serverräumen – Feuerlöschgeräte in Serverräumen – Erstellung eines Backup- und Recoverykonzepts	☒	☐
• Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO); Bei einem physischen oder technischen Zwischenfall sollen personenbezogene Daten rasch wiederhergestellt werden. (Notfallmanagement/ Notfallpläne/ Leitlinie) --- • Umgesetzt durch: (bitte Maßnahme nachfolgend aufführen) – Regelmäßige Prüfung von Backups – Extern gelagerte Backups – Notfallhandbuch	☒	☐
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)		
• Datenschutz-Management; z.B. Datenschutzrichtlinie --- • Umgesetzt durch: (bitte Maßnahme nachfolgend aufführen) – Erstellung und regelmäßige Prüfung Datenschutzkonzept	☒	☐
• Incident-Response-Management; Als neues Schutzziel wird die „Belastbarkeit“ der Systeme und Dienste erwähnt. Gemeint sein könnte, dass Systeme und Dienste einer gewissen Beanspruchung standhalten müssen.	☒	☐

Ins Deutsche übersetzt, passen also eher die Begriffe Resilienz bzw. Widerstandsfähigkeit der Systeme bzw. Dienste, die bereits aus dem Notfallmanagement bekannt sind. --- • Umgesetzt durch: (bitte Maßnahme nachfolgend aufführen) – Vorhalten von aktiven Reserven – Mehrfache redundante Leitungen zwischen Serverräumen – Mehrfache redundante Leitungen zu ISPs		
• Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO); Privacy by Default heißt übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen“ und bedeutet, dass die Werkeinstellungen datenschutzfreundlich auszugestalten sind. Nach dem Grundgedanken sollen insbesondere die Nutzer geschützt werden, die weniger technikaffin und z.B. dadurch nicht geneigt sind, die datenschutzrechtlichen Einstellungen ihren Wünschen entsprechend anzupassen. --- • Umgesetzt durch: (bitte Maßnahme nachfolgend aufführen) –	☐	☒
• Auftragskontrolle Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen. • Umgesetzt durch: (bitte Maßnahme nachfolgend aufführen) – Auftragnehmer hat Datenschutzbeauftragten bestellt – Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart – Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis – Sicherstellung und Vernichtung von Daten nach Beendigung des Auftrages – Laufende Überprüfung des Auftragnehmers und seiner Tätigkeit	☒	☐

Anlage 3 - Unterauftragsverhältnisse

Name	Adresse	Produkt
Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay, D02 R296, Dublin, Irland	Microsoft 365 (Cloud-Kollaborationsplattform, Exchange Online, SharePoint Online, Teams etc.
INSOCAM GmbH	Nußbergstraße 11, 66119 Saarbrücken	AmWin (Gefahrenmeldesoftware der Leitstelle)
Bite AG	Im Köller 3, 70794 Filderstadt	Disponic (Personalplanungssoftware)
cobra - computer's brainware GmbH	Weberinnenstraße 7, 78467 Konstanz	Cobra (CRM Software)
CSS Computer Security Service GmbH	Wilhelm-Beckmann-Straße 7, 45307 Essen	Datix - Wächterkontrollsystem, Einzelarbeitsplatzabsicherung (alt)
DATCOM protelematik GmbH	Sprudelallee 19, 63628 Bad Soden-Salmünster	Geld und Wertransporter (GPS Überwachung, Überfalltaster etc.)
AUREX GmbH	Christophstraße 31, 50670 Köln	Cobra (CRM Software)
1&1 Internet SE	Eigendorfer Str. 57, 56410 Montabaur	E-Mail Empfang