

Vertrag über die Auftragsverarbeitung personenbezogener Daten nach
Art. 28 Abs. 3 der EU Datenschutz-Grundverordnung

zwischen dem/der - nachstehend Auftraggeber genannt -

der Stadt Suhl

und der

..... - nachstehend Auftragnehmer genannt -

Präambel

Der Auftraggeber hat den Auftragnehmer mit Auftrag vom mit der Lieferung, Errichtung, Betrieb, Unterhaltung, Instandhaltung und Versicherung von 3 stationären Verkehrsüberwachungssystemen im Stadtgebiet Suhl beauftragt.

Zur Umsetzung der Regelungen der EU-DGSVO, treffen Auftraggeber und Auftragnehmer im Hinblick auf den Datenschutz die folgenden Regelungen:

§ 1 Gegenstand und Dauer des Auftrags; fristlose Kündigung

- (1) Der Gegenstand des Auftrags ergibt sich aus der Leistungsbeschreibung.
- (2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.
- (3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer das Kontrollrecht des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 2 Konkretisierung des Auftragsinhalts / Art und Zweck der vorgesehenen Verarbeitung von Daten

- (1) Der Auftragnehmer übernimmt für den Auftraggeber die Verarbeitung der mittels der Verkehrsmesssysteme aufgezeichneten Datensätze, sowie Wartungs- und Systembetreuungsarbeiten an den Verkehrsmesssystemen. Diese Wartungsarbeiten erfolgen auch im Wege der Fernwartung.

Bei den Arbeiten haben Mitarbeiter des Auftragnehmers möglicherweise Zugriff auf personenbezogene Daten, die einerseits an den Auftragnehmer zur Bearbeitung übermittelt werden, andererseits auf den Anlagen des Auftraggebers gespeichert sind. Eine Verarbeitung dieser Daten geschieht nur, soweit dies für die Erfüllung der vertraglichen Leistungen unerlässlich ist.

Im Rahmen dieser Auftragsverarbeitung ist der Auftraggeber uneingeschränkt Herr des Verfahrens.

- (2) Die Art der zu verarbeitenden personenbezogenen Daten sind folgende:
 - Digitales Bildmaterial mit Datums-/Zeitstempel, eine Ortscodierung, sowie amtliche Kennzeichen der abgebildeten Kraftfahrzeuge zzgl. technische und organisatorische Parameter der Messung;
 - Namen und Kontaktdaten der Sachbearbeiter beim Auftraggeber
- (3) Betroffene Personenkreise sind:
 - Verkehrsteilnehmer und Fahrzeuginsassen
 - Sachbearbeiter beim Auftraggeber
- (4) 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. DS-GVO erfüllt sind.

§ 3 Technisch-organisatorische Maßnahmen

- (1) Der Auftragnehmer wird die in Anlage 1 aufgeführten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten einhalten und die Einhaltung regelmäßig, wenigstens im Jahresabstand, überprüfen und dokumentieren. Den Nachweis über die Prüfung wird der Auftragnehmer dem Auftraggeber auf Anforderung überlassen.
- (2) 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.
- (3) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO sowie gem. § 64 BDSG herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen (vgl. Anlage 1) 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 DS-GVO zu berücksichtigen.
- (4) Die technischen und organisatorischen Maßnahmen gem. Anlage 1 unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau bzw. die vereinbarten

Standards der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen und für die Dauer des Auftrages aufbewahren. Der Auftragnehmer wird nur solche alternativen technischen und organisatorischen Maßnahmen treffen, bei denen die Ausführung der Vorschriften der DS-GVO in ihren jeweils gültigen Fassungen, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen gewährleistet sind. Der Auftragnehmer berücksichtigt hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik.

§ 4 Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gem. Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich.

§ 5 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 an den Auftraggeber weiterleiten.
- (2) Soweit vom Leistungsumfang in der Leistungsvereinbarung umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 6 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

- (1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
 - (a) Beim Auftragnehmer ist folgende/r Beauftragte/r für den Datenschutz schriftlich bestellt, der/die seine/ihre Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt:

.....
(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

Ein Wechsel des/der Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

- (b) Erstellung und Pflege eines Verzeichnisses über die Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO.
- (c) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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 Verschwiegenheit muss in geeigneter Weise auch für die Zeit nach Beendigung der Beschäftigungsverhältnisse der mit der Verarbeitung beschäftigten Mitarbeiter sichergestellt sein.

- (d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 1).
- (e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- (f) 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.
- (g) 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.
- (h) Der Auftragnehmer 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 Person gewährleistet wird.
- (i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.
- (j) Der Auftragnehmer hat den Auftraggeber über Auskunftersuchen Dritter oder öffentlicher Behörden unverzüglich zu informieren.

Der Auftragnehmer unterstützt den Auftraggeber in seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III DS-GVO. Insbesondere erteilt der Auftragnehmer aller hierfür erforderlichen Auskünfte unverzüglich nach Anforderung durch den Auftraggeber.

Gleiches gilt für Auskunftersuchen sonstiger Dritter oder öffentlicher Behörden, soweit der Auftraggeber zur Auskunftserteilung verpflichtet ist.

§ 7 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 darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher Genehmigung des Auftraggebers beauftragen.

Die dokumentierten technischen und organisatorischen Maßnahmen des Auftragnehmers werden ebenfalls Bestandteil des Vertragsverhältnisses zwischen dem Auftragnehmer und den Unterauftragnehmern.

Die Auslagerung auf Unterauftragnehmer ist nur zulässig, soweit:

- der Auftraggeber dies durch schriftliche Zustimmungserklärung gestattet und
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.
- (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) Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.
 - (6) Eine weitere Auslagerung durch den Unterauftragnehmer an weitere Unterauftragsnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers.
 - (7) In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmers deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragnehmer eingesetzt gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern.
 - (8) Die Weiterleitung von Daten an den Unterauftragnehmer ist erst zulässig, wenn der Unterauftragnehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt.

§ 8 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, beim Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, aber auch unangemeldet,

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 DS-GVO 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, kann insbesondere erfolgen durch
 - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
 - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).
- (4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.
- (5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 9 Mitteilung bei Verstößen des Auftragnehmers

- (1) Der Auftragnehmer erstattet dem Auftraggeber unverzüglich Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen sowie die von ihm eingesetzten Unterauftragnehmer Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.
- (2) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DS-GVO 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, den 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.
- (3) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 10 Weisungsbefugnis des Auftraggebers

- (1) Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.
- (2) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen.
- (3) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (4) 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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 11 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.

§ 12 Sonstiges

- (1) Auf diese Vereinbarung ist ausschließlich das Recht der Bundesrepublik Deutschland anzuwenden, soweit diesem nicht zwingendes Recht der Europäischen Union vorgeht. Die

Anwendung des Übereinkommens der Vereinten Nationen über den internationalen Warenverkehr (CISG) ist ausgeschlossen.

- (2) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so soll hierdurch die Gültigkeit der übrigen Bestimmungen dieses Vertrages nicht berührt werden. Dasselbe gilt für den Fall, dass dieser Vertrag eine Regelungslücke enthält. Die Vertragspartner verpflichten sich, anstelle der unwirksamen oder undurchführbaren Bestimmung oder zur Ausfüllung einer Regelungslücke eine neue Bestimmung zu treffen, die dem am nächsten kommt, was die Vertragspartner ursprünglich vereinbaren wollten oder vereinbart hätten, wenn sie die Regelungslücke erkannt hätten.
- (3) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform und müssen als solche ausdrücklich gekennzeichnet sein. Dies gilt auch für eine Änderung des Schriftformerfordernisses selbst.
- (4) Eine teilweise oder vollständige Übertragung von Rechten und Pflichten aus diesem Vertrag ist jeweils nur mit Einwilligung der anderen Vertragspartei zulässig.

Ort, Datum

Ort, Datum

Stadt Suhl

Auftraggeber

Auftragnehmer

Anlage 1: Technisch-Organisatorische Maßnahmen

Anlage 1

Technische und organisatorische Maßnahmen gemäß DS-GVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**
Alarmanlage, Absicherung von Gebäudeschächten, Sicherheitsschlösser, Einlasskontrolle beim Empfang, Protokollierung der Besucher beim Empfang, Schlüsselregelung für das gesamte Gebäude, sorgfältige Auswahl von Sicherheitspersonal, Tragepflicht von Mitarbeiter-/Gästeausweisen, sorgfältige Auswahl von Reinigungspersonal;
- **Zugangskontrolle**
Authentifizierung mit Benutzername und Passwort, Erstellen von Benutzerprofilen, Einsatz von Antivirussoftware, Firewalls, VPN (extern), SSL , separates VLAN (intern), individuelle Benutzerberechtigungen, Passwortvergabe/Passwortrichtlinie, Personenkontrolle beim Empfang, Protokollierung der Besucher, Codeschloss zum Zutritt in die betreffenden Büros*;
- **Speicherkontrolle**
Keine Maßnahmen erforderlich, da der Auftraggeber keine personenbezogenen Daten eingibt – diese werden automatisiert an der Straße erfasst, Manipulationen wären durch digitale Signatur in der Anlage erkennbar*; Identifikation des Mitarbeiters (AG) im Ticketsystem durch Benutzerlogin
- **Zugriffskontrolle**
Einsatz von Aktenvernichtern, Ordnungsgemäße Vernichtung von Datenträgern, Anzahl der Administratoren auf das Minimum reduziert, Einsatz von Dienstleistern zur Akten- und Datenvernichtung, Berechtigungskonzept für Zugriffsrechte, Passwortrichtlinie (Passwortlänge, Gültigkeitsdauer), sichere Aufbewahrung von Datenträgern, Verwaltung der Benutzerrechte durch Administratoren;
- **Trennungskontrolle**
Logische Trennung von Daten unterschiedlicher Auftraggeber und auch einzelner Messplätze desselben Auftraggebers*;
- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)** findet nicht statt.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle/Transportkontrolle**
Online-Anbindung der Messgeräte per verschlüsselter Verbindung (VPN), Manipulation verhindert durch elektronische Signatur der Vorfallsdaten, Datenaustausch verschlüsselt (TLS)*, Verarbeitung der Daten in separatem Netzwerk (VLAN)*;
- **Übertragungskontrolle**
Logfiles auf Webserver dokumentieren Up- und Download der Daten*, Logfiles auf der Anlage dokumentieren Änderungen durch Service-Nutzer;
- **Eingabekontrolle/Benutzerkontrolle**
Protokollierung der Bearbeiter auf Seiten von Auftraggeber und Auftragnehmer;
- **Datenintegrität**
Wahrung durch Signatur der Vorfallsdateien*.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)** Tägliches Backup*;
- **Zuverlässigkeit**
Verfügbarkeit und ggfs. Entstörung der Systeme wird gewährleistet durch interne ITServices.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- **Datenschutz-Management**
Jährliches internes und externes* Audit, Konzernrichtlinie zur Datensicherheit und zum Datenschutz, regelmäßige Schulung der Mitarbeiter, Verpflichtung auf das Datengeheimnis bei Neueinstellungen;
- **Incident-Response-Management**
Verfahrensanweisungen zur Meldung von Datenpannen an den internen Datenschutzbeauftragten, Information an den Auftraggeber, ggfs. Meldung an Aufsichtsbehörde;
- **Auftragskontrolle**
Beschränkung der Verwendung mobiler Datenträger auf das notwendige Maß, Automatisierte Löschung von Daten nach dem letzten Zugriff, Datenschutzbeauftragter als Ansprechpartner für den Auftraggeber, Gewährleistung der Verarbeitung entsprechend den Weisungen des Auftraggebers durch enge Abstimmung der jeweiligen Ansprechpartner, Vertreterregelung, Erstellung und Pflege eines „Mandantensteckbriefs“ mit den jeweiligen Weisungen des Auftraggebers.

* gilt nur für Datenaufbereitung