

Vereinbarung nach Art 28 DSGVO

zwischen der

Stadt Dortmund

Amt für Stadterneuerung

Kampstraße 47

44122 Dortmund

– Verantwortlicher –

nachstehend „Auftraggeber“ genannt

und dem/der

.....

– Auftragsverarbeiter –

nachstehend „Auftragnehmer“ genannt

Präambel

Der Auftraggeber möchte dem Auftragnehmer den in § 1 Abs. 1 definierten Auftrag erteilen. Teil des Auftrags ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 der europäischen Datenschutzgrundverordnung (DSGVO) stellt bestimmte Anforderungen an eine solche Verarbeitung von personenbezogenen Daten im Wege der Auftragsverarbeitung. Zur Wahrung und Konkretisierung der datenschutzrechtlichen Rechte und Pflichten und der Umsetzung der Anforderungen gemäß Art. 28 DSGVO schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist. Die Regelungen der vorliegenden Vereinbarung (im Folgenden „Vertrag“) gehen im Zweifel den Regelungen des Auftrags vor. Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Auftrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand

Der Gegenstand der Verarbeitung personenbezogener Daten, insbesondere Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer, ergeben sich aus dem Auftrag **XX** auf den hier verwiesen wird (im Folgenden „Auftrag“ genannt) (und, sofern vorhanden, aus der dazugehörigen Leistungsbeschreibung).

(2) Dauer

Die Dauer der Verarbeitung personenbezogener Daten entspricht der Laufzeit des Auftrags. Sobald der Auftrag endet, endet auch diese Vereinbarung, ohne dass es einer gesonderten Kündigung bedarf. Die Beendigung dieser Vereinbarung wird dabei aber solange aufgeschoben, wie der Auftragnehmer noch im Besitz von personenbezogenen Daten aus der beauftragten Verarbeitung ist, oder soweit er noch Zugriffsmöglichkeiten auf solche Daten des Auftraggebers hat.

§ 2 Art und Zweck der Verarbeitung

(1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Auftrag (und der dazugehörigen Leistungsbeschreibung) [Angebot der Fa. **XX** vom **XX**, Leistungsbeschreibung vom **XX**].

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten bzw. Datenkategorien [zutreffendes Ankreuzen / ergänzen]

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
- ☐ ...

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

[zutreffendes Ankreuzen / ergänzen]

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ (interne) Ansprechpartner
- ☐ ...

(4) Die Erbringung der vereinbarten Verarbeitung personenbezogener Daten 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. Der Auftragnehmer verpflichtet sich in diesem Fall dem Auftraggeber die Erfüllung der Voraussetzung der Art. 44 ff. DSGVO nachzuweisen und soweit erforderlich durch Bereitstellung

der notwendigen Informationen an der Erstellung einer Übertragungsrisikobewertung (Transfer Impact Assessment) mitzuwirken.

§ 3 Rechte und Pflichten des Auftragnehmers und des Auftraggebers

(1) Der Auftragnehmer und jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten hat, wird die personenbezogenen Daten ausschließlich im Auftrag und nur auf schriftlich dokumentierte Weisung des Auftraggebers (auch in Bezug auf eine etwaige Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation) verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor dem Beginn der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Dem Auftraggeber obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO, er entscheidet allein über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten.

Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag, den Auftrag (und die Leistungsbeschreibung, sofern sie vorliegt) festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischem Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen über die Art und Weise der Verarbeitung, der Weiterleitung oder Herausgabe, die Berichtigung, Löschung und Sperrung von Daten. Der Auftragnehmer hat, sofern er sich bei einer Verarbeitung auf eine Weisung des Auftraggebers beruft, diese Weisung nachzuweisen.

Kopien oder Duplikate der verarbeiteten 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) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer wird dem Auftraggeber vor Beginn der Verarbeitung der personenbezogenen Daten geeignete Nachweise über die

entsprechende Verpflichtung schriftlich übermitteln oder die gesetzliche Verschwiegenheitspflicht schriftlich darlegen.

Soweit der Auftrag keine Vorgaben über die Notwendigkeit einer Verpflichtung der Beschäftigten nach dem Verpflichtungsgesetz macht, gilt das Folgende: Im Falle einer gesetzlichen Anforderung zu einer Verpflichtung der Angestellten des Auftragnehmers durch den Auftraggeber (z.B. Verpflichtungsgesetz i. V. m. Steuergeheimnis, Sozialdaten oder Personaldaten der Stadtverwaltung, etc.) stellt der Auftragnehmer die Bereitschaft der eingesetzten Beschäftigten zur Verpflichtung sicher.

(3) Der Auftragnehmer verpflichtet sich, alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen zu ergreifen. Hierunter fallen insbesondere die geeigneten technischen und organisatorischen Maßnahmen, um ein dem Risiko der Verarbeitung personenbezogener Daten angemessenes Schutzniveau zu gewährleisten. Die im Rahmen der Beauftragung verarbeiteten Informationen sind gegen die Kenntnisnahme durch Unbefugte, vor Verlust oder unberechtigter Veränderung unter Berücksichtigung des jeweils aktuellen Stands der Technik zu sichern. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen gerecht werden und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzliche, angemessene und spezifische Maßnahmen.

Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen.

Der Auftragnehmer wird dem Auftraggeber vor Beginn der Verarbeitung der personenbezogenen Daten geeignete Nachweise über die entsprechenden, von ihm getroffenen, Maßnahmen schriftlich übermitteln. Hierfür stellt er noch vor Abschluss des Vertrags eine Übersicht über die von ihm umgesetzten technischen und organisatorischen Maßnahmen als Anlage zu diesem Vertrag zur Verfügung. Für die Dauer des Vertrags, ist der Auftragnehmer ebenfalls verpflichtet, Sicherheitsmaßnahmen an den Fortlaufenden Stand der Technik im angemessenen Umfang anzupassen oder diese zu Ändern. Dies setzt jedoch immer voraus, dass durch die Änderung das ursprünglich bestehende Schutzniveau nicht verschlechtert wird.

Der Auftragnehmer stellt soweit erforderlich sicher, dass eine Verarbeitung personenbezogener Daten des Auftraggebers außerhalb seiner Geschäftsräume, insbesondere im Homeoffice oder bei mobiler Arbeit, nur unter Einhaltung geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO erfolgt.

Der Auftragnehmer verpflichtet seine Beschäftigten vertraglich,

- die festgelegten Sicherheitsmaßnahmen einzuhalten,
- die Verarbeitung ausschließlich über die vom Auftragnehmer bereitgestellten

Systeme und Zugänge vorzunehmen,

- keine personenbezogenen Daten des Auftraggebers auf anderen als den hierfür vorgesehen dienstlichen Geräten zu speichern oder dauerhaft in privaten Räumen aufzubewahren.

Der Auftragnehmer stellt sicher, dass Datenbestände des Auftraggebers nicht in privaten Räumen verbleiben. Soweit dies technisch nicht vollständig ausgeschlossen werden kann, trifft der Auftragnehmer ergänzende Maßnahmen (z. B. Verschlüsselung, automatische Löschung, Zugriffsbeschränkungen) und führt interne Kontrollen im Rahmen der arbeitsrechtlichen Bestimmungen durch.

(4) Der Auftragnehmer verpflichtet sich, die in Art. 28 Abs. 2 und 4 DSGVO genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einzuhalten. Dies umfasst insbesondere folgende Bedingungen:

(a) Der Auftragnehmer nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(b) Nimmt der Auftragnehmer die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in der

vorliegenden Vereinbarung festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Der Auftragnehmer stellt als Anlage zu diesem Vertrag eine Übersicht über die eingesetzten weiteren Auftragnehmer bereit, die über Namen und Kontaktinformationen des Auftragnehmers, auch die von diesen übernommenen Tätigkeiten und den Standort des Firmensitzes informiert. Sofern keine eigene Übersicht besteht, wird hierfür das Formular der Anlage genutzt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

Die Weitergabe von personenbezogenen Daten des Auftraggebers durch den Auftragnehmer an den weiteren Auftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller o.g. Voraussetzungen gestattet.

(5) Der Auftragnehmer verpflichtet sich, angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, der Pflicht des Auftraggebers zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person (Betroffenenrechte) nachzukommen. Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber, informiert diesen und wartet dessen Weisungen ab.

(6) Der Auftragnehmer verpflichtet sich, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten rechtzeitig zu informieren und zu unterstützen. Insbesondere bei Störungen, Vorfällen der Informationssicherheit, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Format

informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde.

(7) Der Auftragnehmer verpflichtet sich, nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen und / oder dem Auftraggeber zurückzugeben. Die vorhandenen Kopien wird der Auftragnehmer umgehend löschen, sofern ihn nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten trifft. Gleiches gilt für Test- und Ausschussmaterial. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen und dem Auftraggeber auf dessen Verlangen nachzuweisen.

Der Auftragnehmer ist verpflichtet, auch über das Ende des Auftrags hinaus die ihm im Zusammenhang mit dem Auftrag bekannt gewordenen Daten vertraulich zu behandeln.

(8) Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten vor Beginn der Verarbeitung der personenbezogenen Daten schriftlich zur Verfügung zu stellen. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(9) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen. An der Erstellung des Verarbeitungsverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben rechtzeitig in geeigneter Weise mitzuteilen.

(10) Der Auftragnehmer wird Überprüfungen, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen. Der Auftraggeber wird entsprechende Überprüfungen rechtzeitig gegenüber dem Auftragnehmer

ankündigen. 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. Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit. Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept oder andere geeignete Nachweise für die Auftragsverarbeitung sowie über zugriffsberechtigte und verpflichtete Personen zur Verfügung.

(11) Der Auftragnehmer verpflichtet sich, Art und Zweck der Verarbeitung inkl. KI-Einsatz zu beschreiben und zu konkretisieren. Er ist verpflichtet, die Kategorien der verarbeiteten Daten und die Art der KI-Nutzung (z. B. automatisierte Analyse, Chatbot, Anomalie-Erkennung) anzugeben, zu beschreiben und zu konkretisieren. Er ist weiter verpflichtet, entsprechende Sicherheitsmaßnahmen (z. B. Pseudonymisierung, Zugriffskontrolle, Logging) einzurichten, zu dokumentieren und dem Auftraggeber mitzuteilen. Weiter ist er verpflichtet die bestehenden Unterauftragsverhältnisse (wenn der KI-Dienst Subprozessoren nutzt) offenzulegen, die Unterauftragsverarbeitungsverträge auf Verlangen vorzuzeigen und dem Auftraggeber die entsprechenden Nachweise zu Dokumentations- und Kontrollrechten auf Verlangen vorzuzeigen. Weiter ist der Auftragnehmer bei der KI-Nutzung zur Unterstützung des Auftraggebers bei Betroffenenrechten verpflichtet.

§ 4 Ansprechpartner(in) in Angelegenheiten des Datenschutzes

(1) Die Kontaktdaten der behördlichen Datenschutzbeauftragten des Auftraggebers lauten:

Die Datenschutzbeauftragte

44122 Dortmund

Tel.: 0231 / 50 24999

datenschutz@stadtdo.de

(2) Der Auftragnehmer wird vor Beginn der Verarbeitung der personenbezogenen Daten dem Auftraggeber schriftlich die Kontaktdaten seiner Ansprechpartnerin / seines Ansprechpartners in Angelegenheiten des Datenschutzes mitteilen. Soweit der Auftragnehmer durch gesetzliche Regelungen zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, umfasst diese Mitteilung die Kontaktdaten des Datenschutzbeauftragten.

§ 5 Außerordentliches Kündigungsrecht des Auftrags

Der Auftraggeber kann den in § 1 Abs. 1 genannten Auftrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus dieser Vereinbarung nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder einer Weisung des Auftraggebers nicht nachkommt. Bei einfachen (also weder vorsätzlichen noch grob fahrlässigen) Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 6 Schlussbestimmungen

(1) Der Auftraggeber und der Auftragnehmer sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist. 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, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

(2) Mündliche Nebenabreden zu dieser Vereinbarung existieren nicht. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Dortmund

Ort, Datum

Ort, Datum

Unterschrift

Unterschrift

Anlage 1: Übersicht der Unterauftragnehmer Auftragsnehmers (TOM's)

Anlage 2: Technische und organisatorische Maßnahmen des Auftragsnehmers (TOM's)

Anlage 3: Standardvertragsklauseln (soweit für die Verarbeitung im Drittland erforderlich)

Beispiel für Technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes und der -sicherheit

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

- Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
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;

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

- Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

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

- 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;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.