

Vereinbarung zur Auftragsverarbeitung nach Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen der Verbraucherzentrale Nordrhein-Westfalen e.V., Mintropstr. 27, 40215 Düsseldorf, vertreten durch den Vorstand Wolfgang Schuldzinski

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

...

- Auftragsverarbeiter - nachfolgend Auftragnehmer genannt.

Präambel

Im Rahmen der zwischen Auftraggeber und Auftragnehmer bestehenden Hauptvereinbarung verarbeitet der Auftragnehmer personenbezogene Daten des Auftraggebers in der Art, dass dabei ein Zugriff des Auftragnehmers auf personenbezogene Daten des Auftraggebers nicht ausgeschlossen werden kann.

Diese Auftragsverarbeitung im Sinne von Art. 28 DSGVO wird durch die nachfolgende Vereinbarung entsprechend den gesetzlichen Vorschriften konkretisiert und geregelt.

Es gelten die Begriffsbestimmungen der DSGVO.

Diese Vereinbarung wird mit ihrer Unterzeichnung wesentlicher Bestandteil der zugrunde liegenden Hauptvereinbarung. Gleiches gilt für alle Anlagen, auf die diese Vereinbarung ausdrücklich Bezug nimmt.

Andere zwischen den Parteien getroffene datenschutzrelevante Vereinbarungen, die ebenfalls für die hier geregelte Auftragsverarbeitung gelten, gehen dieser Vereinbarung nur dann vor, wenn sie die Regelungen dieser Vereinbarung weiter ausführen. Andere Vereinbarungen zwischen den Parteien, die den Kerngehalt der Bestimmungen dieser Vereinbarung verändern oder hinter dem hier vereinbarten Datenschutzniveau zurück bleiben, werden von dieser Vereinbarung verdrängt.

1. Gegenstand und Dauer der Auftragsverarbeitung

Gegenstand und Dauer der Auftragsverarbeitung richten sich grundsätzlich nach den Regelungen der zugrunde liegenden Hauptvereinbarung.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind.

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien der betroffenen Personen sind in Anlage 1 beschrieben.

Der Auftraggeber hat das Recht zur fristlosen Kündigung aus wichtigem Grund, wenn der Auftragnehmer datenschutzrechtliche Vorschriften oder ihm nach dieser Vereinbarung obliegende Pflichten erheblich verletzt.

Eine erhebliche Pflichtverletzung liegt insbesondere dann vor, wenn die Pflichtverletzung zur Folge hat, dass der Auftraggeber seinen gesetzlichen Verpflichtungen als datenschutzrechtlich verantwortliche Stelle nicht nachkommen kann oder der Auftragnehmer einer Weisung des Auftraggebers nicht nachkommen kann oder will.

2. Umfang der Weisungsbefugnisse des Auftraggebers

Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und damit alleine zuständig für die Beurteilung der Zulässigkeit dieser Auftragsverarbeitung sowie für die Wahrung der Rechte der Betroffenen.

Der Auftraggeber hat das Recht, dem Auftragnehmer hinsichtlich der Auftragsverarbeitung Weisungen zu erteilen. Eine Weisung im Sinne dieser Vereinbarung ist eine einseitige Anordnung des Auftraggebers gegenüber dem Auftragnehmer, die auf einen bestimmten Umgang mit personenbezogenen Daten bei der Auftragsverarbeitung gerichtet ist. Die Erteilung von Weisungen hat in Schriftform oder per E-Mail zu erfolgen.

Auskünfte an Dritte oder an Betroffene darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

3. Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, regelmäßig beim Auftragnehmer in dessen Geschäftsbetrieb durch Stichproben, die in der Regel rechtzeitig anzumelden sind, die Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO, der Bestimmungen dieser Vereinbarung und der aufgrund derer erteilten Weisungen sowie insbesondere die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen zu überprüfen. Der Auftraggeber hat das Recht, diese Kontrollen auch durch Dritte vornehmen zu lassen.

4. Pflichten des Auftragnehmers

Der Auftragnehmer hat neben den in dieser Vereinbarung getroffenen Regelungen zusätzlich die Pflichten gemäß Art. 28 bis 33 DSGVO. Dies sind insbesondere die nachfolgend dargestellten Vorgaben.

4.1 Datenverarbeitung

Der Auftragnehmer darf die personenbezogenen Daten des Auftraggebers nur im Rahmen dieser Vereinbarung und der dazu ergangenen dokumentierten Weisungen des Auftraggebers verarbeiten, es sei denn, dass er gesetzlich zu einer anderen Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 S. 2 lit. a DSGVO). Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

Der Auftragnehmer verwendet die Daten, die ihm im Rahmen der Erfüllung dieses Vertrags bekannt geworden sind, nur für die vereinbarten Vertragszwecke. Eine Verarbeitung oder Nutzung ohne Kenntnis des Auftraggebers oder zu eigenen Zwecken des Auftragnehmers ist nicht erlaubt. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die der Einhaltung gesetzlicher Aufbewahrungsfristen dienen.

4.2 Beauftragter für den Datenschutz

Sofern der Auftragnehmer gesetzlich dazu verpflichtet ist (Art. 37 DSGVO, § 38 BDSG), hat er einen Beauftragten für den Datenschutz zu bestellen. Auf Verlangen des Auftraggebers hat er diesem dessen Kontaktdaten zu nennen und die Bestellung unter Vorlage einer Kopie der Bestellungsurkunde nachzuweisen. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

4.3 Vertraulichkeit

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrags fort.

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.

Auf Weisung des Auftraggebers hat der Auftragnehmer die von ihm mit der Auftragsverarbeitung betrauten Personen auch auf weitere Vertraulichkeitsgebote (z. B. Fernmeldegeheimnis und Postgeheimnis) zu verpflichten, soweit dies gesetzlich gefordert ist.

4.4 Kontrollen durch den Auftragnehmer

Der Auftragnehmer hat durch geeignete und regelmäßige Kontrollen der internen Prozesse sowie der technischen und organisatorischen Maßnahmen sicherzustellen, dass bei der Auftragsverarbeitung nicht gegen Datenschutzvorschriften, die Regelungen dieser Vereinbarung oder die zugehörigen Weisungen verstoßen wird. Das Ergebnis der Kontrollen ist zu dokumentieren.

4.5 Kontrollen beim Auftragnehmer durch Datenschutzaufsichtsbehörden

Über Kontrollen und Maßnahmen der Datenschutzaufsichtsbehörden beim Auftragnehmer ist der Auftraggeber unverzüglich zu informieren, soweit die in dieser Vereinbarung geregelte Auftragsverarbeitung davon berührt ist. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeiten- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten im Auftrag beim Auftragnehmer ermittelt.

4.6 Unterstützung des Auftraggebers

Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeiten- 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.

Auch bei der Erfüllung der Rechte betroffener Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, zur Meldung von Datenpannen, zu erforderlichen Datenschutz-Folgenabschätzungen und zu vorherigen Konsultationen mit der Aufsichtsbehörde hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen.

4.7 Mitzuteilende Verstöße des Auftragnehmers

Der Auftragnehmer und die bei ihm beschäftigten Personen haben den Auftraggeber bei Störungen des Verarbeitungsablaufs, bei Verdacht auf Datenschutzverletzungen oder Verstößen gegen die in dieser Vereinbarung getroffenen Festlegungen und anderen Unregelmäßigkeiten bei der Auftragsverarbeitung unverzüglich zu informieren. Dies gilt in besonderem Maße im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und 34 DSGVO.

Gleichmaßen hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren, 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. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

4.8 Duldung von Kontrollen durch den Auftraggeber

Der Auftragnehmer ist verpflichtet, Kontrollen gemäß Ziffer 3 dieser Vereinbarung zu dulden und den Auftraggeber bei deren Durchführung zu unterstützen. Er hat dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, 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), durch Vorlage eines schlüssigen Datensicherheitskonzepts oder vertragliche Zusicherungen.

4.9 Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten

Die Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten erfolgt durch den Auftragnehmer nur dann, wenn er dazu entsprechende dokumentierte Weisungen des Auftraggebers erhalten hat.

Sollte sich eine betroffene Person unmittelbar an den Auftragnehmer wegen der Berichtigung, Löschung oder Sperrung seiner Daten wenden, so wird der Auftragnehmer dieses Begehren unverzüglich an den Auftraggeber weiterleiten, der dann bezüglich des weiteren Vorgehens entscheidet.

Beim Auftragnehmer im Rahmen der Auftragsverarbeitung anfallendes Test- und Ausschussmaterial ist dagegen unverzüglich durch den Auftragnehmer zu vernichten. Bis zur Vernichtung ist dieses Material gesichert aufzubewahren. Die Vernichtung hat mit einem Verfahren zu erfolgen, das dem Stand der Technik entspricht.

Soweit der Auftragnehmer im Rahmen der Prüfung oder Wartung von automatisierten Verfahren und Datenverarbeitungsanlagen des Auftraggebers defekte oder nicht mehr benötigte Datenspeicher ausbaut, sind diese beim Auftragnehmer gesichert aufzubewahren, bis sie einer Reparatur, Entsorgung oder weiteren Verwendung zugeführt worden sind. Vor einer Weitergabe der Komponenten an Dritte hat der Auftragnehmer sicherzustellen, dass alle darauf gespeicherten Daten des Auftraggebers physisch gelöscht sind. Diese Verfahrensweise ist auch einzuhalten, wenn der Auftragnehmer im Rahmen der Auftragsverarbeitung von ihm genutzte Datenspeicher ausbaut, soweit diese Daten des Auftraggebers enthalten.

5. Technische und organisatorische Maßnahmen

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.

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.

Bezüglich der technischen und organisatorischen Maßnahmen, die im Rahmen dieses Vertragsverhältnisses als verbindlich festgelegt werden, wird auf Anlage 2 verwiesen. Alternativ kann dieser Vereinbarung auch ein durch den Auftragnehmer vorgelegtes und vom Auftraggeber akzeptiertes Sicherheitskonzept als Anlage 2 beigefügt werden, sofern dieses die Vorgaben von Art. 32 DSGVO angemessen umsetzt.

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 in dokumentierter Form (schriftlich oder elektronisch) mit dem Auftraggeber abzustimmen.

6. Unterauftragsverhältnisse

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 Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Einsatz von Unterauftragnehmern bedarf der vorherigen schriftlichen bzw. dokumentierten Zustimmung des Auftraggebers. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Unterauftragnehmers mitteilt. Der Auftragnehmer hat den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem ergriffenen technischen und organisatorischen Maßnahmen im Sinn von Art. 32 DSGVO sorgfältig auszuwählen. Die relevanten Prüfungsunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Der Auftragnehmer hat die vertraglichen Vereinbarungen mit den Unterauftragnehmern so zu gestalten, dass sie den Bestimmungen dieser Vereinbarung und der dazu erteilten Weisungen zwischen Auftraggeber und Auftragnehmer entsprechen. Im 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. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragnehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Auf Verlangen des Auftraggebers hat der Auftragnehmer Einsicht in die bestehenden Vereinbarungen mit den Unterauftragnehmern zu gewähren.

Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

Der Auftragnehmer hat die Einhaltung der Pflichten des Unterauftragnehmers zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragnehmer den Datenschutzverpflichtungen nachkommt, die ihm durch den Auftragnehmer im Einklang mit den Bestimmungen dieser Vereinbarung vertraglich auferlegt wurden.

Die derzeit eingesetzten Unterauftragnehmer sind in Anlage 1 zu dieser Vereinbarung abschließend aufgeführt.

7. Beendigung der Auftragsverarbeitung

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 gelangte 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.

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.

8. Schlussbestimmungen

Unabhängig von der Verpflichtung des Auftragnehmers, personenbezogene Daten gemäß den Vorschriften der DSGVO und sonstiger datenschutzrechtlicher Vorschriften, gemäß den Bestimmungen dieser Vereinbarung und der aufgrund derer erteilten Weisungen zu verarbeiten, ist der Auftragnehmer zudem auch zur Vertraulichkeit im Hinblick auf Betriebs- und Geschäftsgeheimnisse des Auftraggebers verpflichtet. Diese Verpflichtung gilt für alle betrieblichen und geschäftlichen Angelegenheiten sowie sonstige Informationen, über die der Auftragnehmer im Rahmen der Auftragsverarbeitung Kenntnis erlangt und die ihrer Natur nach vertraulich zu behandeln sind. Der Auftragnehmer hat bezüglich dieser Informationen gegenüber unbefugten Dritten Stillschweigen zu bewahren. Etwaige weitergehende Regelungen, die im zugrundeliegenden Hauptvertrag getroffen wurden, bleiben unberührt. Die Verpflichtung zur Wahrung der Vertraulichkeit gilt über das Vertragsende hinaus.

Es gilt deutsches Recht.

Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

Ort und Datum

Ort und Datum

Auftraggeber

Auftragnehmer

Anlage 1 - Auftragspezifische Vereinbarungen

1. Gegenstand und Dauer der Auftragsverarbeitung

Bezüglich Gegenstand und Dauer der Auftragsverarbeitung wird auf die Hauptvereinbarung verwiesen.

2. Art und Zweck der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Art und Zweck der Datenverarbeitung:

...

Art der personenbezogenen Daten:

...

Kategorien betroffener Personen:

...

3. Unterauftragsverhältnisse

Als Unterauftragnehmer werden derzeit seitens des Auftragnehmers folgende Unternehmen (Firma, Anschrift, im Rahmen der Auftragsverarbeitung wahrgenommene Tätigkeit) oder freien Mitarbeiter (Name, Anschrift, im Rahmen der Auftragsverarbeitung wahrgenommene Tätigkeit) eingesetzt:

...

Anlage 2 - Technische und organisatorische Maßnahmen

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. Pfortner, 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)**

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 entsprechenden 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 Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z. B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen