

Vertrag über die Auftragsdatenverarbeitung nach Art. 28 DS-GVO

zwischen

und

Firma

Druckerei Mack GmbH & Co. KG

Straße

Friedenstraße 9

Ort

D-97638 Mellrichstadt

- Verantwortlicher -

Nachstehend **Auftraggeber** genannt

- Auftragsverarbeiter -

Nachstehend **Auftragnehmer** genannt

§ 1 Einleitung, Geltungsbereich, Definitionen

- (1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
- (2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
- (3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

§ 2 Gegenstand und Dauer der Verarbeitung

- (1) **Gegenstand**
Der Auftragnehmer übernimmt folgende Verarbeitungstätigkeiten:
Produktion und Versand von Druckdienstleistungen jeglicher Art, ggf. Datenerstellung, -aufbereitung oder -korrektur
- (2) **Dauer**
Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von einem Monat zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

(1) Art und Zweck der Verarbeitung

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Datenerhebung, -verarbeitung oder -nutzung zum Zwecke der Herstellung, der Auslieferung, der Rechnungsstellung und ggf. Personalisierung der Druckdaten.

(2) Art der Daten

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien

(durch den Auftraggeber anzugeben)

- Personenstammdaten
- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Empfänger und Versender von Nachrichten, die an die Auftraggeberin gerichtet sind oder von dieser ausgehen

(3) Kategorien der betroffenen Personen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

(durch den Auftraggeber anzugeben)

- Kunden
- Abonnenten
- Beschäftigte i. S. d. § 3 Abs. 11 BDSG
- Lieferanten
- Handelsvertreter
- Ansprechpartner
- Empfänger und Versender von Nachrichten, die an die Auftraggeberin gerichtet sind oder von dieser ausgehen

§ 4 Anwendungsbereich und Verantwortlichkeit

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
- (2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.
- (3) Ziehen Einzelweisungen Mehrkosten nach sich, insbesondere wenn diese über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind diese dem Auftragnehmer zu vergüten.

§ 5 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
- (2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten (Anlage 1) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
- (3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten gegen Erstattung der dem Auftragnehmer hierdurch entstehenden, nachzuweisenden Aufwände und Kosten.
- (4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
- (5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die

erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

- (6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

Verantwortlicher im Sinne der Datenschutz-Grundverordnung, sonstiger in den Mitgliedstaaten der Europäischen Union geltenden Datenschutzgesetze und anderer Bestimmungen mit datenschutzrechtlichem Charakter ist die:

Druckerei Mack GmbH & Co. KG
Friedenstraße 9
97638 Mellrichstadt
Deutschland
Tel.: 09776 8121-0
E-Mail: info@mack-druck.de
Website: <https://www.mack-druck.de>

- (7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
- (8) Der Auftragnehmer berichtet oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
- (9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
- (10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 6 Pflichten des Auftraggebers

- (1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §5 Abs. 10 entsprechend.
- (3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 7 Anfragen betroffener Personen

- (1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.
- (2) Bei der Erbringung der Unterstützungsleistungen nach Abs. 1 dem Auftragnehmer entstehenden und nachzuweisenden Aufwände und Kosten sind vom Auftraggeber zu ersetzen.

§ 8 Nachweismöglichkeiten

- (1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Können auch konkrete Arten von Nachweisen genannt werden bzw. zum Nachweis der Einhaltung der vereinbarten Pflichten, kann der Auftragnehmer, dem Auftraggeber folgende Informationen zur Verfügung vorlegen:
 - ✓ Durchführung eines Selbstaudits
- (2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Der Auftragnehmer erhält vom Auftraggeber eine Aufwandsentschädigung für seinen im Rahmen dieser Kontrollen nachzuweisenden anfallenden Kosten.

Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 9 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 schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
- (3) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
 - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
 - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.
- (4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (5) 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.
- (6) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);
sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 10 Haftung

- (1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.
- (2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.
- (3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.
- (4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

§ 11 Sonderkündigungsrecht

- (1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers

gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

- (2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
- (3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.
- (4) Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Auftraggeber entstehen.

§ 12 Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- (3) Für Nebenabreden ist die Schriftform erforderlich.
- (4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

Ort, Datum

Auftraggeber

Mellrichstadt, 02.10.2018

Ort, Datum



Auftragnehmer

Anlage 1

Allgemeine technische und organisatorische Maßnahmen

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

a) Zutrittskontrolle

Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.

Den Zutritt zu unserem Firmengebäude stellen wir durch folgenden Maßnahmen sicher:

- Manuelles Schließsystem
- Schlüsselregelung / Liste
- Empfang / Rezeption
- Besucher ausschließlich in Begleitung durch Mitarbeiter
- Sorgfalt bei Auswahl Reinigungsdienste

b) Zugangskontrolle

Eine unbefugte Systemnutzung ist zu verhindern.

Um den Zugang zu unserem Netzwerk zu schützen, haben wir folgende Maßnahmen getroffen:

- Login mit Benutzername + Passwort
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Firewall
- Einsatz VPN bei Remote-Zugriffen
- Automatische Desktopsperre
- Verschlüsselung von Notebooks / Tablet
- Verwalten von Benutzerberechtigungen
- Richtlinie „Sicheres Passwort“

c) Zugriffskontrolle / Benutzerkontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein.

Um unerlaubte Tätigkeiten innerhalb der Systeme der Druckerei Mack GmbH & Co. KG außerhalb der eingeräumten Berechtigungen zu verhindern, haben wir folgende Maßnahmen getroffen:

- Rechtevergabe nach Rollen / Organisationseinheiten
- Verwaltung der Zugriffsrechte durch Administrator
- Minimale Anzahl an Administratoren
- Datenschutzkonforme Entsorgung von Datenträgern und Papier
- Mobile Datenträger enthalten keine personenbezogenen Daten

d) Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden.

Um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden, haben wir die folgenden Maßnahmen getroffen:

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Mandantenfähigkeit relevanter Anwendungen

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DS-GVO, Art. 25 Abs. 1 EU-DS-GVO)

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

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

a) Weitergabekontrolle / Übertragungskontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

Folgende Maßnahmen haben wir in Bezug auf die Weitergabe von personenbezogenen Daten getroffen:

- Sichere Aufstellung von Servern / NAS
- Unternehmenseigene Domain zur E-Mail-Kommunikation (intern)
- Weitergabe an Dritte nur nach Prüfung der Rechtsgrundlage
- Schriftliche Festlegung der Weitergabe in Drittländer
- Sichere Übertragung von Datenlieferungen (SFTP, VPN)

- Beschränkung des zur Übermittlung befugten Personenkreises

b) Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Nachvollziehbarkeit innerhalb der Datenverwaltung stellen wir wie folgt sicher:

- Protokollierung der Eingabe personenbezogener Daten

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

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

- Feuerlöscher Serverraum
- Serverraum klimatisiert
- USV
- RAID System / Festplattenspiegelung
- Kontrolle des Sicherungsvorgangs
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

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

- a) Datenschutz-Management
- b) Incident-Response-Management
- c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DS-GVO)
- d) Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers

- Vertragliche Regelungen gemäß § 11 BDSG (Auftragsdatenverarbeitung)
- Unteraufträge nur bei gleichwertigem Schutzniveau
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln