

Anlage

Vertrags-Nr.:

Vereinbarung zur Auftragsdatenverarbeitung

zwischen

- Auftraggeber -

und

Druck H. Buschhausen GmbH

Westerholter Straße 777

45701 Herten

- Auftragnehmer -

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsdatenverarbeitungsverhältnis gemäß § 11 Bundesdatenschutzgesetz (BDSG) eingegangen bzw. erfolgt die in der Leistungsvereinbarung niedergelegte Verarbeitung der Daten im Auftrag des Auftraggebers (sog. Auftragsverarbeitung). Um die Rechte und Pflichten aus dem Auftragsdatenverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

Die Regelungen des BDSG treten am 25.05.2018 außer Kraft, weshalb bei der Erstellung dieser Vereinbarung bereits die Erfordernisse der DSGVO beachtet wurden. Dabei ersetzen die Regelungen und Begriffe der DSGVO ab Inkrafttreten der DSGVO die Regelungen des BDSG.

1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Auftraggeber die gemäß § 3 Abs. 7 BDSG verantwortliche Stelle (Art. 4 Nr. 7 DSGVO Verantwortlicher) ist.

2 Begriffsbestimmung

- 2.1 Diese Vereinbarung bezieht sich nur auf die Verarbeitung personenbezogener Daten nach den vom Auftraggeber (Verantwortlichen) vorgegebenen Weisungen.
- 2.2 Verarbeitung meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
- 2.3 Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
- 2.4 Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- 2.5 Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (z.B. Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Bestehende Weisungen (z.B. durch diese Vertragsergänzung) können vom Auftraggeber danach durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

3 Konkretisierung des Auftragsinhalts

- 3.1 Der Gegenstand und die Dauer der Auftragsdatenverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten sind in der Leistungsvereinbarung niedergelegt.
- 3.2 Die Art der verwendeten personenbezogenen Daten ist im **Anhang 2 („Konkretisierung der Datenkategorien“)** konkret beschrieben.
- 3.3 Der Kreis der durch den Umgang mit den personenbezogenen Daten Betroffenen ist im **Anhang 3 („Konkretisierung der von der Verarbeitung Betroffenen“)** konkret beschrieben.

4 Verantwortlichkeit und Weisungsbefugnis

- 4.1 Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (§ 3 Abs. 7 BDSG / Art. 4 Nr. 7 DSGVO). Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen (§ 11 Abs. 2 S. 2 Nr. 4 und 10 BDSG / Art. 28 Abs. 3 lit. g DSGVO) soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und anhand der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Erfüllung unterstützen (Art. 28 Abs. 3 lit. f DSGVO).
- 4.2 Der Auftragnehmer darf Daten ausschließlich im Rahmen der dokumentierten Weisungen des Auftraggebers verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen unverzüglich diese rechtlichen Anforderungen vor der Verarbeitung mit. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Auftraggeber danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (§ 11 Abs. 2 S. 2 Nr. 9 BDSG / Art. 28 Abs. 3 lit. a DSGVO).
- 4.3 Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG / Art. 28 Abs. 3 DSGVO zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- 4.4 Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in den in Ziffer 4.2 dieser Vereinbarung genannten Umfangs.
- 4.5 Der Auftraggeber führt das Verfahrensverzeichnis gem. § 4g Abs. 2 Satz 2 BDSG / Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO. Der Auftragnehmer stellt dem

Auftraggeber auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnissverzeichnis zur Verfügung.

- 4.6 Die Verarbeitung und Nutzung der Daten im Auftrag des Auftraggebers findet ausschließlich auf dem Gebiet der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraumes (EWR) statt. Eine Verlagerung in einen Staat außerhalb der EU bzw. des EWR bedarf der vorherigen Zustimmung des Auftraggebers. Die besonderen Voraussetzungen der §§ 4b, 4c BDSG / Art. 44 bis 49 DSGVO bleiben unberührt.
- 4.7 Eine Verarbeitung von personenbezogenen Daten in Privatwohnungen der Mitarbeiter des Auftragnehmers (Telearbeitsplätze, Heimarbeitsplätze) ist nicht zulässig, es sei denn, es handelt sich um notwendige Dienstleistungsfälle im Rahmen der Bereitschaftsregelungen des Auftragnehmers und es werden geeignete technische und organisatorische Maßnahmen zum Schutz der Daten des Verantwortlichen getroffen, die denen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen und das Schutzniveau der in Anhang 1 dargestellten technischen und organisatorischen Maßnahmen nicht unterschreiten.

5 Beachtung zwingender gesetzlicher Pflichten durch den Auftragnehmer

- 5.1 Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den Auftragnehmer gemäß § 11 Abs. 4 BDSG / Art 28 Abs. 3, Art. 30 DSGVO die nachfolgenden gesetzlichen Pflichten.
- 5.2 Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 BDSG (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Datenschutzrechts eingewiesen worden sind. Eine den § 5 BDSG entsprechende Verpflichtung der Arbeitnehmer des Auftragnehmers wird auch nach Außerkrafttreten des Bundesdatenschutzgesetzes beibehalten. Dies umfasst auch die Belehrung über die in diesem Auftragsdatenverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.
- 5.3 Der Auftragnehmer hat nach Maßgabe des § 4f BDSG / Art. 37 DSGVO einen betrieblichen Datenschutzbeauftragten bestellt, der seine Tätigkeit gemäß §§ 4f und 4g BDSG / Art. 38 und Art 39 DSGVO ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitzuteilen.
- 5.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden nach § 38 BDSG / Art. 58 DSGVO oder falls eine Aufsichtsbehörde nach §§ 43, 44 BDSG / Art. 83 DSGVO bei dem Auftragnehmer ermittelt. Darüber hinaus teilt der Auftragnehmer dem Auftraggeber unverzüglich mit, wenn er wegen eines Verstoßes gegen die DSGVO auf Schadensersatz verklagt wird und sodann in regelmäßigen Abständen.
- 5.5 Der Auftragnehmer verpflichtet sich mit Inkrafttreten der DSGVO zur Führung eines Verzeichnisses zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung (Art. 30 Abs. 2 DSGVO). Dieses Verzeichnis enthält mindestens
- (a) den Namen und die Kontaktdaten des Auftragnehmers und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

- (b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- (c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- (d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO.

Der Auftragnehmer gewährt dem Auftraggeber auf Anfrage binnen 14 Tagen nach schriftlicher Aufforderung Einsicht in die diese Verarbeitung betreffenden Informationen des Verzeichnisses.

6 Sicherheit der Verarbeitung und deren Kontrolle

- 6.1 Die Vertragsparteien vereinbaren die in dem **Anhang 1 „Technische und organisatorische Maßnahmen“** zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG / Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Der Anhang ist Gegenstand dieser Vereinbarung.
- 6.2 Technische und organisatorische Maßnahmen berücksichtigen zum Zeitpunkt des Abschlusses dieser Vereinbarung den Stand der Technik und unterliegen jeweils dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technische und organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.
- 6.3 Der Auftragnehmer verpflichtet sich, die konkreten technischen und organisatorischen Maßnahmen auf deren Wirksamkeit im Hinblick auf die Sicherheit der Verarbeitung in regelmäßigen Abständen zu überprüfen, zu bewerten und diese Risikobewertung zu dokumentieren.
- 6.4 Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Aufgrund der Kontrollverpflichtung des Auftraggebers gemäß § 11 Abs. 2 Satz 4 BDSG / Art. 28 Abs. 1, Abs. 3 DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG sowie die Durchführung der regelmäßig durchgeführten Risikobewertung gemäß Ziffer 6.3 nach. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats oder von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) erbracht werden.
- 6.5 Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des

Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen (§ 11 Abs. 2 S. 2 Nr. 7 BDSG / Art. 28 Abs.3 lit. h DSGVO).

7 Mitteilung bei Verstößen durch den Auftragnehmer

7.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich nach Feststellung schwerwiegender Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (§ 11 Abs. 2 S. 2 Nr. 8 BDSG / Art. 28 Abs. 3 lit. c, Art. 33, Art 34 DSGVO). Dabei hat die Unterrichtung mindestens folgenden Inhalt:

- (a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- (b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- (c) eine Beschreibung der bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Können nicht alle in Ziffer 7.1. lit. a – lit. c genannten Informationen zum Zeitpunkt der Unterrichtung zur Verfügung gestellt werden, so sind die Informationen unverzüglich nach Kenntnis, ggf. schrittweise zur Verfügung zu stellen.

7.2 Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

8 Löschung und Rückgabe von Daten

8.1 Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

8.2 Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftraggeber, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten (§ 11 Abs. 2 S. 2 Nr. 10 BDSG / Art. 28 Abs. 3 lit. g DSGVO). Gleiches gilt für Test- und Ausschussmaterial. Ein Lösungsprotokoll ist dem Auftraggeber auf Anforderung vorzulegen.

8.3 Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu

seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

9 Subunternehmer

- 9.1 Der Auftragnehmer beauftragt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte schriftliche Genehmigung des Auftraggebers und verpflichtet sich nur Subauftragnehmer unter Beachtung der nachstehenden Voraussetzungen einzusetzen:
- 9.1.1 Der Auftragnehmer wählt den Subunternehmer sorgfältig aus und prüft vor der Beauftragung, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach § 9 BDSG / Art. 32 Abs. 1 DSGVO geeigneten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser, sofern gesetzlich gefordert, einen betrieblichen Datenschutzbeauftragten i.S.d. § 4f BDSG / Art. 37 DSGVO bestellt hat.
- 9.1.2 Der Auftragnehmer gestaltet die vertraglichen Vereinbarungen mit dem / den Subunternehmer/n so, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- 9.2 Nicht als Subunternehmer im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
- 9.3 Zum Zeitpunkt der Vertragsunterzeichnung beauftragte Unterauftragnehmer werden in **Anhang 4 („Genehmigte Subunternehmer“)** einschließlich der Verarbeitungsstandorte und der Art der Dienstleistung dokumentiert. Die in dieser Liste genannten Unterauftragnehmer gelten als von Anfang an rechtmäßig beauftragt im Sinne von Ziffer 9 Abs. 1, sofern die Umsetzung der dort genannten Voraussetzungen durch den Auftragnehmer gewährleistet wird.
- 9.4 Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn auch der Unterauftragnehmer die Pflichten des Auftragnehmers aus diesem Vertrag erfüllt bzw. dies gegenüber dem Auftragnehmer zugesichert hat und der Auftragnehmer die Einhaltung dieser Pflichten durch den Unterauftragnehmer regelmäßig überprüft.

10 Nebenleistungen

Die Ziffern 1 bis 8 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

11 Vertraulichkeit und Datenschutzkontrolle

- 11.1 Der Auftraggeber und der Auftragnehmer verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen vertraulich zu behandeln. Dies gilt für den in der Leistungsvereinbarung vereinbarten Zeitraum und auch über die Beendigung der Einzelaufträge bzw. der Geschäftsbeziehung hinaus.
- 11.2 Der Auftragnehmer verpflichtet sich, dem betrieblichen Datenschutzbeauftragten des Auftraggebers zur Erfüllung seiner jeweiligen gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren.

12 Schlussbestimmungen

- 12.1 Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Das Schriftformerfordernis gilt nicht, soweit dieses zwischen den Vertragsparteien aufgrund einer ausdrücklichen und individuellen Vereinbarung aufgehoben wird.
- 12.2 Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:
- 1) Anhang 1 „Technische und organisatorische Maßnahmen“
 - 2) Anhang 2 „Konkretisierung Datenarten / Datenkategorien“
 - 3) Anhang 3 „Konkretisierung der von der Verarbeitung Betroffenen“
 - 4) Anhang 4 „Genehmigte Subunternehmer“
 - 5) Anhang 5 „Angaben zur Konkretisierung der Hauptleistung / des Auftragsinhalts“

Auftraggeber

Vertretungsberechtigter

Auftragnehmer

Druck H.Buschhausen GmbH

Heinz-Dirk Buschhausen
Vertretungsberechtigter

Anhang 1 bitte vom Auftragnehmer ausfüllen lassen!

Anhang 1 „Technisch-organisatorische Maßnahmen“ nach § 9 BDSG/ Art. 28 Abs. 3 lit. c, 32 DSGVO

Ziffer 6 der Vereinbarung zur Auftragsdatenverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Datenschutzmaßnahmen auf diesen Anhang.

1 Technische und organisatorische Sicherheitsmaßnahmen

Gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG/ Art. 28 Abs. 3 lit. c, 32 DSGVO sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

3 Innerbetriebliche Organisation des Auftragnehmers

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

4 Konkretisierung der Einzelmaßnahmen

Im Einzelnen werden folgende Maßnahmen bestimmt:

1. Zutrittskontrolle

Der Zutritt in die Geschäftsräume der Firma Druck H. Buschhausen GmbH wird durch folgende Maßnahmen gesichert:

- Alarmanlage
- Manuelles Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal

2. Zugangskontrolle

Die Zugangskontrollen erfolgt im Hause Druck H. Buschhausen GmbH Software folgenmaßen:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort

- Zuordnung von Benutzerprofilen zu IT-Systemen
- Sicherheitsschlösser
- Sorgfältige Auswahl von Reinigungspersonal
- Verschlüsselung von mobilen Datenträgern
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall

3. Zugriffskontrolle

Die Zugriffskontrollen werden im Hause Druck H. Buschhausen GmbH Software folgenderweise hergestellt:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

4. Weitergabekontrolle

Die Übergabe bzw. Bereitstellung der Daten des Auftraggebers erfolgt unter folgenden Maßnahmen:

- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –Fahrzeugen

5. Eingabekontrolle

Es werden grundsätzlich keine Dateneingaben im Rahmen der Layoutarbeiten durchgeführt.

6. Auftragskontrolle

Vor Auftragsvergabe wurden folgende Punkte geprüft:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. Verfügbarkeitskontrolle

Die Systemverfügbarkeit wird unter folgenden Maßgaben hergestellt:

- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Notfallplans
- Serverräume nicht unter sanitären Anlagen

8. Trennungsgebot

Die Trennung der Systeme wird im Hause Druck H. Buschhausen GmbH grundsätzlich hergestellt und mit folgenden Maßnahmen unterstützt

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Archivsystem

Anhang 2 und Anhang 3 bitte vom Auftraggeber ausfüllen!

Anhang 2 Konkretisierung der „Datenkategorien“ gemäß Ziffer 3.2

Anhang 3 Konkretisierung der von der Verarbeitung Betroffenen gemäß Ziffer 3.3

Anhang 4 bitte vom Auftragnehmer ausfüllen lassen!

Anhang 4 „Genehmigte Subunternehmer“ gemäß Ziffer 9.3

Subunternehmer Firma, Anschrift	Verarbeitungsstandort Anschrift	Art der Dienstleistung
Diakonisches Werk im Kirchenkreis Recklinghausen	Alte Grenzstraße 90 45663 Recklinghausen	kuvertieren von Mailingaktion Lettershoparbeiten

Anhang 5 bitte vom Auftraggeber ausfüllen!

Anhang 5 Angaben zur Konkretisierung der Hauptleistung / des Auftragsinhalts (mangels schriftlicher Leistungsvereinbarung gemäß Ziffer 3.1)

1 Gegenstand des Auftrags

2 Dauer des Auftrags

Der Auftrag ist bis auf Widerruf erteilt.

3 Umfang, Art und Zweck der vorgesehenen Datenverarbeitung

Umfang: Satz- und Layoutarbeiten, Gestaltung von Akzidenzien, Versand von Mailings
eine Erhebung von personenbezogenen Daten findet nicht statt.

Art: Speicherung von Firmendaten, Adressedaten, Telefon und E-Mail, Inhaber, usw.

Mitarbeiterdaten, Name, Telefon und E-Mail z.B. Für Visitenkarten

Drucken von gelieferten Adressedaten (Name, Straße, PLZ und Ort) für die Postadressierung von Mailings und Postsendungen.

Zweck: Erstellung von Drucksachen jeder Art, Mailing- und Lettershoparbeiten