Rahmenvereinbarung

zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Stand 10. März 2018

Anlage „Einzelbeauftragung“ als Ergänzung zu dieser Rahmenvereinbarung notwendig.

zwischen der/dem Auftraggeber (Verantwortlicher)

Firma	
Firma	
Straße/Nr.	
PLZ/Ort	

und dem Auftragnehmer (Auftragsverarbeiter)

Firma	LETTERservice Herbert Rodemeier
Straße/Nr.	Lägenfeldstr. 8
PLZ/Ort	30952 Ronnenberg

1. Gegenstand und Dauer des Auftrags

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Die ordnungsgemäße und datenschutzgerechte Erledigung richtet sich nach dem jeweiligen Einzelauftrag.

Die Inhalte dieser Vereinbarung gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Diese Rahmenvereinbarung umfasst die ordnungsgemäße und datenschutzgerechte Erledigung folgender Arbeiten:

- **IT-Dienstleistungen**
  allgemeine Datenaufbereitung auf Weisung des Kunden
  postalische Korrekturen
  Abgleiche mit Fremdadressen
  Selektionen
  Portooptimierungen
  Druckaufbereitung
- **Druck-Dienstleistungen**
  Variabler Datendruck
  Personalisierung
  Direktadressierung
- **Lettershop-Leistungen**
  Konfektionierung
  Postauflieferung

Der genaue Umfang der zu erledigenden Arbeiten richtet sich nach der jeweiligen Einzelbeauftragung als Ergänzung zu dieser Rahmenvereinbarung.

Dauer des Vertrages zur Auftragsverarbeitung:

- Die Dauer (Laufzeit) dieser Rahmenvereinbarung wird auf unbestimmte Zeit geschlossen. Die Kündigungsfrist beträgt 4 Wochen zum Monatsende. Die Möglichkeit zur fristlosen Kündigung bleibt davon unberührt.

2. Konkretisierung des Auftragsinhalts

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

Gegenstand der Verarbeitung personenbezogener Daten sind unter anderem folgende Datenarten bzw. -kategorien:

- Adressdaten
- Personenstammdaten

- Kommunikationsdaten
- Rechnungsdaten
- Bankdaten
- Gesundheitsdaten

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen unter anderem:

- Kunden
- Beschäftigte i. S. d. § 3 Abs. 11 BDSG und deren Familienangehörige
- Interessenten
- Mitglieder
- Rechnungsempfänger
- Daten aus öffentlichen Quellen

Die genauen Datenarten, Datenkategorien sowie betroffene Personenkreise richten sich nach der jeweiligen Einzelbeauftragung als Ergänzung zu dieser Rahmenvereinbarung.

3. Technisch-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. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen (**Einzelheiten in Anlage 1**)**.**

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 zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Als (externer) Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau:

  Thomas Trümper, Berater Datenschutz
  Krausenstraße 33, 30171 Hannover
  Telefon 0511 7602120, Mobil 01590 1238182
  Mail info@truemper-datenschutz.de
  Web https://www.truemper-datenschutz.de

  bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

- Zur Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO setzt der Auftragnehmer bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

- Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (**Einzelheiten in Anlage 1**).

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

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

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

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

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.

Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Die weisungsbefugten Personen des Auftraggebers werden dem Auftragnehmer im Vorfeld schriftlich mitgeteilt.

Weisungsempfänger beim Auftragnehmer sind:

- Herbert Rodemeier
- Birgit Kutschenreuter
- Yvonne Poteri

- Tina Engel
- Tanja Richter
- Karen Aselmann

Eine Änderung der Weisungsempfänger wird dem Auftraggeber unverzüglich schriftlich mitgeteilt.

10. Löschung und Rückgabe von personenbezogenen Daten

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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.

11. Übermittlung der Auftragsdaten

Die elektronische Übermittlung personenbezogener Daten im Rahmen dieser Vereinbarung, erfolgt ausschließlich in verschlüsselter Form.

Der Auftragnehmer stellt hierzu dem Auftraggeber einen geschützten https-Server zur Verfügung.

Wünscht der Kunde einen Versand per E-Mail, wird dieser von Seiten des LETTERservice Herbert Rodemeier ausschließlich verschlüsselt erfolgen.

Wichtiger Hinweis:

Die Sicherung der Daten bei der Übertragung (Weitergabekontrolle) muss dem Stand der Technik entsprechen, um ein dem Risiko entsprechendes Schutzniveau zu gewährleisten. Eine Übertragung von unverschlüsselten Daten im Zusammenhang mit einen unverschlüsselten Übertragungsverfahren entspricht nicht dem Stand der Technik und stellt demnach einen Verstoß gegen das BDSG und die DSGVO dar.

Im Rahmen der Datenminimierung (Art. 5 Abs. c DS-GVO) stellt der Auftraggeber sicher, dass ausschließlich die Daten an den Auftragnehmer übermittelt werden, die für die Zwecke der Verarbeitung erforderlich sind.

11. Sonstiges

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme durch Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren.

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

11. Übermittlung der Auftragsdaten

Die elektronische Übermittlung personenbezogener Daten im Rahmen dieser Vereinbarung, erfolgt ausschließlich in verschlüsselter Form.

Der Auftragnehmer stellt hierzu dem Auftraggeber eine eigene „Private Cloud“ mit End-to-End-Verschlüsselung zur Verfügung. Die Dateien werden beim Auftragnehmer direkt verschlüsselt auf einen Server abgelegt.

Wünscht der Kunde einen Versand per E-Mail, wird dieser von Seiten des LETTERservice Herbert Rodemeier ausschließlich mit kennwortgeschütztem Downloadlink zur Private Cloud, das Kennwort wird mit separater Email versendet.

> **Wichtiger Hinweis:**
>
> Die Sicherung der Daten bei der Übertragung (Weitergabekontrolle) muss dem Stand der Technik entsprechen, um ein dem Risiko entsprechendes Schutzniveau zu gewährleisten. Eine Übertragung von unverschlüsselten Daten im Zusammenhang mit einem unverschlüsselten Übertragungsverfahren entspricht nicht dem Stand der Technik und stellt demnach einen Verstoß gegen das BDSG und die DSGVO dar.

Im Rahmen der Datenminimierung (Art. 5 Abs. c DSGVO) stellt der Auftraggeber sicher, dass ausschließlich die Daten an den Auftragnehmer übermittelt werden, die für die Zwecke der Verarbeitung erforderlich sind.

11. Sonstiges

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme durch Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren.

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

Änderungen und Ergänzungen dieser Vereinbarung 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.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der sonstigen Vereinbarungen nicht.

Es gelten die allgemeinen Geschäftsbedingungen des Auftragnehmers.

Gerichtsstand ist der Sitz des Auftragnehmers.

Ort, Datum	Stempel | Unterschrift **Auftraggeber**
Ort, Datum	Stempel | Unterschrift **Auftragnehmer**

LETTERservice
Herbert Rodemeier

Anlage I

Rahmenvertrag zur Auftragsverarbeitung

technische & organisatorische Maßnahmen

Stand 12. März 2018

Auftragnehmer

Letterservice Herbert Rodemeier

Lägenfeldstr. 8

30952 Ronnenberg

Ansprechpartner

Thomas Trümper

externer betrieblicher Datenschutzbeauftragter

info@truemper-datenschutz.de

www.truemper-datenschutz.de

1. Grundsätzliches

1.1. Beschreibung der durchzuführenden Aufgaben

Ergibt sich aus dem Vertrag zur Auftragsverarbeitung zwischen LETTER**service** Herbert Rodemeier (Auftragnehmer) und dem Auftraggeber.

1.2. Art der betroffenen Daten

Ergibt sich aus dem Vertrag zur Auftragsverarbeitung

1.3. Erfüllungsort

- In den Räumen des Auftraggebers
- In den Räumen des Auftragnehmers

1.4. Welche Datenübertragungswege sollen genutzt werden?

- Datenträgeraustausch
- Beleghaft/papierhaft
- Datentransfer (verschlüsselt)

2. Organisatorische Fragen

2.1. Ist ein Datenschutzbeauftragter bestellt und liegt eine Bestellungsurkunde vor?

Ja (seit dem 01. Oktober 2014)

2.2. Sind alle Mitarbeiter nachweislich auf die Verschwiegenheit inkl. Fernmeldegeheimnis (§ 88 TKG) verpflichtet worden?

Ja

2.3. Sind alle Mitarbeiter nachweislich auf andere Geheimniswahrung verpflichtet?

Ja (Arbeitsvertrag)

2.4. Werden die Mitarbeiter regelmäßig zu Datenschutzthemen geschult?

Ja

2.5. Werden regelmäßig unabhängige Sicherheitsprüfungen durch eine externe Stelle durchgeführt?

Ja (externer Datenschutzbeauftragter)

2.6. In welchen Staaten wird die Datenverarbeitung (inkl. Fernwartung etc.) durchgeführt?

Deutschland

3. Technische und organisatorische Maßnahmen

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

- **Zutrittskontrolle**
  Das Firmengelände wird nachts durch ein abgeschlossenes Tor gesichert. Die Firmenräume sind durch eine Einbruchmeldeanlage gesichert, die nach DIN/VDE

0833 projektiert wurde. Die Einbruchmeldeanlage besitzt eine Weiterschaltung zu einem Wachunternehmen. Der Zugang zum Gebäude ist stets geschlossen und kann von außen nur mit Sicherheitsschlüsseln geöffnet werden. Die Mitarbeiter haben jeweils einen Schlüssel. Für ausgegebene Schlüssel existiert eine Quittung. Besucher müssen Klingeln und werden von einer Mitarbeiterin oder einem Mitarbeiter persönlich abgeholt. Organisatorisch ist geregelt, dass Fremde sich im Gebäude niemals allein aufhalten oder bewegen dürfen.

- **Zugangskontrolle**
  Der Zugang von außen zu unseren EDV-Systemen ist durch eine wirksame Firewall geschützt. Der Virenscanner wird mehrmals täglich auf neueste Signaturen aktualisiert. Sämtliche PC-System sind passwortgeschützt. Die Passwörter müssen aus mindestens 7 alphanummerischen Zeichen bestehen. Nach 3 Fehleingaben wird der User gesperrt. Für vergebene Passwörter wird eine Passwort-Chronik vorgehalten. Das minimale Kennwortalter beträgt 1 Tag, dass maximale 1 Monat.

- **Zugriffskontrolle**
  Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zurückgreifen. Ausscheidende Mitarbeiter werden mit dem Ausscheiden als User gesperrt. Die EDV-Administrierung erfolgt durch einen externen EDV-Dienstleister. Die User erhalten Support über eine Help-Desk-Anfrage per Mail. User, die nach fehlerhafter Passwort-Eingabe gesperrt sind, können frühestens nach 30 Minuten einen erneuten Anmeldeversuch unternehmen oder werden nach vorherigem Kontakt mit dem Administrator wieder freigeschaltet.

- **Trennungskontrolle**
  Jeder Kunde besitzt ein eigenes Verzeichnis. Innerhalb der jeweiligen Verzeichnisse werden für jeden Auftrag neue Auftragsordner angelegt. Durch diese Trennung wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene bzw. gespeicherte Kunden-Daten getrennt verarbeitet werden können.

3.2. Integrität (Art. 32. Abs. 1 lit. B DS-GVO)

- **Weitergabekontrolle**
  Der Versand der personenbezogenen Daten kann über einen geschützten https-Server abgewickelt werden, welcher der LETTERservice Herbert Rodemeier seinen Kunden zur Verfügung stellt. Wünscht der Kunde einen Versand per E-Mail, wird dieser von Seiten des LETTERservice Herbert Rodemeier ausschließlich verschlüsselt erfolgen. Ausschussmaterial aus der Produktion, welches personenbezogene Daten oder sonstige sensiblen Daten enthält, wird in einem verschlossenen Behälter gesammelt und einem Fachbetrieb zur datenschutzgerechten Entsorgung übergeben.

- **Eingabekontrolle**
  Auf dem Auftragsdeckblatt wird dokumentiert, wenn Adressdaten auf unserem Server gespeichert werden. Weiterhin ist dort ersichtlich, wohin und von wem Adressdaten gespeichert wurden. Veränderungen an Adressdaten (Dubletten entfernen, Adressen postalisch bereinigen) werden auf dem Auftragsdeckblatt und durch das Abspeichern unterschiedlicher Fertigungsstufen dokumentiert.

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

- **Verfügbarkeitskontrolle**
  Unsere EDV-Systeme sind durch RAID-Systeme vor Datenverlust geschützt. Eine unterbrechungsfreie Stromversorgung sorgt bei Stromausfall für ein kontrolliertes Herunterfahren des Servers. Werktägliche Datensicherungen garantieren, dass bei Verlust der Funktionsfähigkeit von EDV-Systemen keine Daten verloren gehen. Für den Fall von Feuer oder anderen EDV-System schädigenden Ereignissen sind die Datensicherungsbänder außerhalb des Serverraumes in einem geeigneten Aufbewahrungsbehälter gelagert. Durchführung von Tests zur Rücksicherung von Nutzerdaten.

- **Rasche Wiederherstellbarkeit**
  Der Vorgang zur Wiederherstellung ist durch einen externen Dienstleister abgedeckt. Die Wiederherstellung (Hardware/Software) liegt bei ca. 24h- 48h.

3.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 und Abs. 2 DS-GVO)

- **Datenschutz-Management**
  Sämtliche datenschutzrelevanten Themen werden durch unseren externen betrieblichen Datenschutzbeauftragten in einem gemeinsamen Datenschutz-Portal (TCDP Schutzklasse III) abgelegt. Hierbei ist der grundsätzliche Umgang in einer Unternehmensrichtlinie dokumentiert. Die einzelnen Maßnahmen werden in einem Datenschutz-Pflichtenheft abgebildet und die Ergebnisse in einer entsprechenden gleichnamigen Ordnerstruktur dokumentiert. In dem Datenschutz-Pflichtenheft werden auch die für die Umsetzung benötigen Fachabteilungen mit den verantwortlichen Mitarbeitern sowie sonstige benötigte Personen/Stellen aufgeführt. Die Sensibilisierung der Mitarbeiter zum Thema Datenschutz wird durch regelmäßige Gespräche, entsprechende Schulungsunterlagen (in den Bereichen Mitarbeiter, Führungskräfte, EDV/IT und HR) sowie einer unregelmäßig erscheinenden Mitarbeiterzeitung (Datenschutz und Datensicherheit) gewährleistet.

- **Incident-Response-Management**
  Monitoring durch externen Dienstleister von:
  - Firewall

- Virenschutz (zentrales Management über den Server – einschließlich Überwachung der Clients)
- Backup
- Server Betriebssystem (Festplattenausfall, verfügbarer Speicher)

Direktmeldung durch externen Dienstleister an den Inhaber. Ggf. Meldung (nach Rücksprache mit dem Inhaber) durch den externen Dienstleister an das Bundesamt für Sicherheit in der Informationstechnik (BSI)

- **Auftragskontrolle**
  Die zur Verarbeitung eingereichten Daten werden entsprechend der gesetzlichen Vorschriften nur im Rahmen der Weisungen des jeweiligen Auftraggebers verarbeitet und insbesondere auch nicht unbefugt an Dritte weitergegeben. Der Weisungsrahmen ist insbesondere durch den schriftlich geschlossenen Rahmenvertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO unter Berücksichtigung der Pflichtinhalte eindeutig vorgegeben. Gleiches gilt für auftragsbezogene Auskünfte. Diese werden an den Auftraggeber weitergeleitet oder im Rahmen seiner Weisungen erteilt.

  - - -
  2018-03-26

Einzelbeauftragung zur Rahmenvereinbarung über die „Auftragsverarbeitung“ gem. Art. 28 DS-GVO

Auftraggeber

Auftragnehmer
Letterservice Herbert Rodemeier
Lägenfeldstraße 8
30952 Ronnenberg

1. Gegenstand der Vereinbarung

☒ Adressdaten-Bearbeitung
- Datenaufbereitung
- Postalische Korrekturen
- Abgleich mit Fremdadressen
- Dublettenabgleich
- Selektionen

☒ Druck
- Druckaufbereitung
- Personalisierung / Adressierung
- Varialbler Datendruck
- Direktadressierung

☒ Lettershop-Leistungen
- Portooptimierung
- Kuvertierung
- Paketversand
- Postauslieferung

2. Dauer der Einzelbeauftragung

☒ Unbefristeter Vertrag
☐ Einzelauftrag zu Auftrag
☐ Regelmäßiger Versand
☐ Befristeter Einzelauftrag bis

3. Art der personenbezogenen Daten

☒ Adressen mit Ansprechpartner
- Firma, Vorname, Nachname
- Adresse
- Geschlecht / Anrede
- Akademischer Grad
- Kommunikationsdaten

☐ Weitere persönliche Daten
- Alter / Geb. Datum
- Bankdaten
- Rechnungsdaten
- Personalstammdaten
- Gesundheitsdaten

Individuelle Daten
☐
☐
☐
☐
☐

4. Kategorien der betroffenen Personen

☒ Kunden / Mitglieder
☒ Interessenten
☒ Werbeadressen
☐ Mitarbeiter
☐ Fremdadressen
☐

5. Unterauftragnehmer

☐

6. Datenübermittlung

☐ https-Server des Auftraggebers
☐ Datenträger (CD/DVD/, USB, HD)
☒ Private Cloud (Auftragnehmer)
☐
☐
☐
☐

Wichtiger Hinweis:
Die Sicherung der Daten bei der Übertragung (Weitergabekontrolle) muss dem Stand der Technik entsprechen, um ein dem Risiko entsprechendes Schutzniveau zu gewährleisten. Eine Übertragung von unverschlüsselten Daten im Zusammenhang mit einem unverschlüsselten Übertragungsverfahren entspricht nicht dem Stand der Technik und stellt demnach einen Verstoß gegen das BDSG und die DSGVO dar.

Ort/Datum

Stempel/Unterschrift Auftraggeber