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