Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO

Datenschutzvereinbarung zwischen

B+M Baustoff + Metall Handels-GmbH
Ziegeleistraße 12
86368 Gersthofen
Deutschland

nachstehend Auftraggeber (Verantwortlicher)

und

rapidmail GmbH
Augustinerplatz 2
79098 Freiburg i.Br.
Deutschland

nachstehend Auftragnehmer (Auftragsverarbeiter)

Es ist Wille der Parteien, dass alle Voraussetzungen und Anforderungen an eine rechtskonforme Auftragsverarbeitung nach der DSGVO und dem BDSG erfüllt oder geschaffen werden.

1. Gegenstand und Dauer des Auftrags

Gegenstand des Vertrages ist die Verarbeitung von Adressdaten des Auftraggebers zur Versendung von Newslettern per E-Mail und transaktionalen E-Mails.

Die Einzelheiten der Leistungen ergeben sich aus den Allgemeinen Geschäftsbedingungen (https://www.rapidmail.de/agb), welche bei der Registrierung vom Auftraggeber akzeptiert werden. Auf diese Leistungen wird hier verwiesen (im Folgenden auch zusammenfassend „Leistungsvereinbarung“). Die Laufzeit des vorliegenden Vertrages richtet sich nach der Leistungsvereinbarung und den dortigen Kündigungsfristen. Eventuell bestehende Verträge zur Auftragsdatenverarbeitung werden durch den Abschluss des vorliegenden Vertrages ersetzt.

2. Konkretisierung des Auftragsinhalts

Umfang, Art und Zweck der Datenverarbeitung ergeben sich aus der Nutzung von Adress- und Personendaten zur Versendung von Newslettern per E-Mail und transaktionalen E-Mails, sowie der Erstellung von personenbezogenen Empfängerstatistiken. Im Übrigen ergeben sich Umfang, Art und Zweck der Verarbeitung personenbezogener Daten auch ausreichend deutlich aus der Leistungsvereinbarung.

Gegenstand der Verarbeitung sind personenbezogene Kundendaten des Auftraggebers. Die durch die Verarbeitung ihrer personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen sind Kunden, Geschäftskontakte und Interessenten des Auftraggebers. Die verarbeiteten Arten von Daten, sowie die Kategorien betroffener Personen ergeben sich im Einzelnen aus dem folgenden Abschnitt.

Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede (teilweise) Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln usw.).

Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind insbesondere nachfolgende Datenkategorien:

- ☒ Namen (Vorname, Nachname)
- ☒ Kontaktdaten (Telefonnummer, E-Mail Adresse)
- ☐ Adressdaten
- ☐ Andere

Kreis der Betroffenen

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

- ☒ Beschäftigte gemäß § 26 Abs. 8 BDSG n.F.
- ☒ Kunden
- ☐ Interessenten
- ☒ Abonnenten
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Andere

3. Technisch-organisatorische Maßnahmen

Die Umsetzung der in der Anlage 1 dargelegten „Technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO“ durch den Auftragnehmer vor Beginn der Verarbeitung wird in einem IT-Sicherheitskonzept dokumentiert, das der Auftraggeber auf Anfrage einsehen kann. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Die Dokumentation des IT-Sicherheitskonzeptes enthält Darlegungen zu allen gemäß Art. 32 DSGVO notwendigen Maßnahmen nach den allgemein anerkannten Schutzzielen der IT-Sicherheit, insbesondere der Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit usw. Dabei wird ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau beachtet.

Die Verarbeitung von Daten in Privatwohnungen ist nur mit Zustimmung des Auftraggebers im Einzelfall gestattet, soweit damit das dauerhafte physische Vorhalten von Daten des Auftraggebers auf Datenträgern in der Privatwohnung verbunden ist. Zulässig ist jedoch die temporäre Zwischenspeicherung durch den Einsatz von mobilen Geräten (z.B. Laptops, Tablet-PCs, Smartphones etc.), sofern die mobilen Geräte über ausreichende, den anerkannten Standards entsprechende Sicherungseinrichtungen (z.B. VPN-Anbindung, Festplattenverschlüsselung etc.) verfügen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung, so dass es dem Auftragnehmer gestattet ist, adäquate Alternativmaßnahmen umzusetzen. Dabei wird das Sicherheitsniveau der festgelegten Maßnahmen insgesamt nicht unterschritten. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer wird Daten, die im Auftrag verarbeitet werden, nur nach Weisung des Auftraggebers berichtigen, löschen oder sperren. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der Betroffenen nach Art. 12 bis 22 DSGVO ist der Auftraggeber verantwortlich. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.

5. Pflichten des Auftragnehmers

Dem Auftragnehmer obliegen die nachfolgenden Pflichten nach Art. 28, 29 DSGVO:

- Die Wahrung der Vertraulichkeit (Datengeheimnis). Alle Personen, die auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf die Vertraulichkeit (Datengeheimnis) verpflichtet sowie über besondere Datenschutzpflichten, Weisungsbefugnisse und die Zweckbindung der Daten belehrt werden.
- Die Umsetzung, Einhaltung und Nachweisbarkeit aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 32, 24 DSGVO. Hierzu kann der Auftragnehmer ergänzend auch aktuelle Berichte oder Prüfungen externer Instanzen (z.B. Datenschutzbeauftragter, IT-Dienstleister, Wirtschaftsprüfer usw.) verwenden.

- Bestellung eines Datenschutzbeauftragten, soweit gesetzlich vorgeschrieben. Als Datenschutzbeauftragte(r) des Auftragnehmers ist bei Vertragsschluss bestellt:

  Frau Teresa Wurst, rapidmail GmbH, Augustinerplatz 2, 79098 Freiburg
  Telefon: 0761 55 77 55 100 | Fax: 0761 58 20 066
  Bitte stellen Sie Ihre Anfrage per E-Mail an **datenschutz@rapidmail.de**

  Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

- Die Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörden, soweit personenbezogene Daten des Auftraggebers betroffen sind. Dies gilt auch, soweit eine zuständige Behörde beim Auftragnehmer ermittelt.

- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen bei möglichen Unterauftragnehmern.

- Der Auftragnehmer wirkt nach Maßgabe des Art. 28 Abs. 3 lit. f DSGVO bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO gegebenenfalls gegen Kostenerstattung mit. Er hat dem Auftraggeber die erforderlichen Angaben und Dokumente auf Anfrage offen zu legen.

- Der Auftragnehmer führt ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und unterstützt den Auftraggeber bei der Erfüllung seiner Dokumentationspflichten gegebenenfalls gegen Kostenerstattung nach Art. 30 DSGVO.

- Der Auftragnehmer unterstützt den Auftraggeber, gegebenenfalls gegen Kostenerstattung, gemäß Art. 28 Abs. 3 lit. e DSGVO nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Person nach Kapitel 3 DSGVO erfüllen kann, z.B. die Information und Auskunft an den Betroffen, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch.

6. Unterauftragsverhältnisse

Soweit bei der Verarbeitung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, ist dies unter folgenden Voraussetzungen zulässig:

- Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit Zustimmung des Auftraggebers gestattet, welche für die in **Anlage 2** aufgeführten Unterauftragnehmer erteilt wird.

- Vor der beabsichtigten Inanspruchnahme weiterer Unterauftragnehmer oder der Ersetzung bereits genehmigter Unterauftragnehmer informiert der Auftragnehmer den Auftraggeber innerhalb angemessener Frist im Voraus. Wenn der Auftraggeber nicht binnen zehn Tagen Einspruch gegen die Heranziehung des Unterauftragnehmers erhebt, gilt die Heranziehung als genehmigt. Im Falle des Einspruchs durch den Auftraggeber steht dem Auftragnehmer ein zweiwöchiges Sonderkündigungsrecht bezüglich der gesamten Leistungsvereinbarung zu.

- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- Der Auftraggeber ist auf schriftliche Anforderung berechtigt, Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

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.

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, eine angemessene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch rechtzeitig vorher anzumeldende Kontrollen, von der Einhaltung dieser Vereinbarung, auch im Geschäftsbetrieb des Auftragnehmers, zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Unterlagen verfügbar zu machen.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet dem Auftraggeber Meldung, wenn Verstöße gegen Datenschutzvorschriften oder vertragliche Vereinbarungen, die dem Schutz der personenbezogenen Daten des Auftraggebers dienen, vorgefallen sind.

Dem Auftragnehmer ist bekannt, dass der Auftraggeber nach Art. 33, 34 DSGVO verpflichtet ist, Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und unverzüglich, möglichst binnen 72 Stunden den Aufsichtsbehörden bzw. im Falle hoher Risiken der betroffenen Person zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragnehmer den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DSGVO bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem Auftraggeber ohne Ansehen der Verursachung unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- eine Beschreibung der Art der Verletzung, der Kategorien und ungefähren Anzahl der betroffenen Personen und personenbezogenen Datensätze,
- Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

- eine Beschreibung der wahrscheinlichen Folgen der Verletzung,
- eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach Art. 33, 34 DSGVO treffen, wird der Auftragnehmer ihn hierbei unterstützen.

9. Weisungsbefugnis des Auftraggebers

Der Umgang mit den personenbezogenen Daten erfolgt im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung des Auftraggebers erteilen.

Die Datenverarbeitung erfolgt nur auf Weisung des Auftraggebers, es sei denn, der Auftragnehmer ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung dieser Daten verpflichtet (z.B. bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht untersagt.

Der Auftragnehmer verwendet die Daten nur für die vereinbarten Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Vertragsdurchführung oder die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Der Auftragnehmer hat den Auftraggeber unverzüglich 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 einen Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche eventuell noch in seinem Besitz befindlichen personenbezogenen Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, soweit die Daten nicht dem Nachweis der auftrags- und ordnungsgemäßen Leistungserbringung oder gesetzlichen Aufbewahrungspflichten unterliegen.

Am 25.09.2018 elektronisch unterschrieben von Michael Reinbold

Anlage 1: Technische und organisatorische Maßnahmen nach Art. 32, 24 DSGVO

Anlage 2: Liste der Unterauftragnehmer

MEGASPACE Internet Service GmbH
Max-von-Laue-Str. 2b
76829 Landau / Pfalz
Deutschland

Amtsgericht Landau / Pfalz,
HRB 3295 USt-Id Nr. DE 219866171

Die durch Megaspace erbrachte Leistung ist das Hosting der Server an Standorten innerhalb der Bundesrepublik Deutschland.

Anlage 1
Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Bei Fragen zur rapidmail Informationssicherheit wenden Sie sich bitte an:

rapidmail GmbH
Datenschutzbeauftragte
Teresa Wurst
Augustinerplatz 2
79098 Freiburg i.Br.
Deutschland

Telefon: 0761 55 77 55 100
Fax: 0761 58 20 066
E-Mail: datenschutz@rapidmail.de

1. Zutritts-/Gebäudesicherheit

Unbefugten ist der Zutritt zu IT-Systemen mit personenbezogenen Daten zu verwehren, insbesondere Legitimation der Berechtigten

- Zutrittskontrollsystem, Chipkarte, kontrollierte Schlüsselausgabe, codierte Schlüssel
- Haupteingang über codierte Schlüssel zu öffnen
- elektrische Türöffner mit Gegensprechanlage und Bildübertragung
- Glastür für Sichtkontakt
- Empfangsbereich besetzt innerhalb Geschäftszeiten, Besucherüberwachung
- Richtlinie zur Begleitung von Besuchern in Gebäuden
- Sicherheitsdienst, nur nachts
- getrennte Sicherheitsbereiche (Server/RZ getrennt von normalen Büroräumen, in separaten Räumlichkeiten und gesondert zutrittsgeschützt)
- gesicherte Fenster im RZ/Serverraum (z.B. vergittert, Sicherheitsglas usw.)
- Videoüberwachung im Serverraum

2. Vertraulichkeit, Integrität, Belastbarkeit

Es ist zu verhindern, dass IT-Systeme von Unbefugten genutzt werden können, insbesondere Benutzeridentifikation und Authentifizierung

- Arbeitsplatzsperren, IT-Systeme und Anwendungen durch komplexe Passwörter geschützt. Festplatten komplett verschlüsselt mittels TrueCrypt
- Passwort-Richtlinien und Komplexitätsanforderungen der Passwörter nach anerkannten Standards (Mindestlänge, Sonderzeichen, regelmäßiger Wechsel des Passworts usw.)
- Schutz der Rechner durch Bildschirmschoner mit Kennwort
- Sperrung des Benutzerkontos nach fehlgeschlagenen Anmeldeversuchen
- revisionssicheres Verfahren zur Rücksetzung „vergessener“ Passwörter
- Rollenmanagement, Identifikation und Authentifikation der Benutzer
- Einrichtung eines Benutzerstammsatzes pro Nutzer
- Verschlüsselung von Datenträgern

3. Berechtigungskonzept

Es ist auf Basis eines Rechte- und Rollenkonzeptes zu gewährleisten, dass Nutzer von IT-Systemen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, insbesondere funktionsbezogene und rollenbasierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung

- dokumentierte Rechteverwaltung
    - unterschiedliche Zugriffsberechtigungen, Protokollierung der Zugriffe, schriftliche Regelungen der Befugnisse
    - dokumentierte Vergabe, regelmäßige Überprüfung und Entziehung der Zugriffsrechte
- Nutzer können nur gemäß den ihnen erteilten Berechtigungen auf personenbezogene Daten zugreifen
- Administrationskonzept vorhanden

4. Übertragungssicherheit, Verschlüsselung

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, insbesondere Transport- und Datenträgerverschlüsselung

- Verschlüsselung der Datenträger (Festplatten) und Datenübertragung
- E-Mail-Kommunikation mit TLS Verschlüsselung
- Anhänge auf Wunsch per sicherer Datenaustauschplattform / Secure File Transfer
- Versand kennwortgeschützter Dateien
- Verschlüsselung mobiler Geräte, gesonderte Arbeitsanweisung für Umgang mit Datenträgern am Arbeitsplatz (Workstation Security). Es sind keine USB-Sticks / mobile Festplatten gestattet
- Nutzung https-Verbindung, VPN-Anbindung
- rechtssichere Vernichtung von Datenträgern nach DIN 66399
- Kein Postversand von sensiblen Daten
- Botentransport durch Auftragnehmer oder Auftraggeber
- Vollständigkeits- und Richtigkeitsprüfung

5. Eingabekontrolle, Änderungshistorie

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle), insbesondere Änderungshistorie

- Protokollierung der Eingaben/Änderungen für alle Mitarbeiter durch Protokollierungssystem mit Auswertungsmöglichkeiten
- Alle relevanten Nutzeraktivitäten werden protokolliert
- Protokollierung der Administrationstätigkeiten, Dienstleistertätigkeiten

6. Datenschutzorganisation, Auftragskontrolle

Es ist zu gewährleisten, dass die Verarbeitung personenbezogener Daten, auch wenn sie im Auftrag erfolgt, den Datenschutzbestimmungen entspricht und dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können, insbesondere Auftrags- und Organisationskontrolle

- Bestellung eines Datenschutzbeauftragten
- Erfüllung der Dokumentations- und Rechenschaftspflichten, insbesondere Verfahrensverzeichnis
- schriftliche Vertragsgestaltung, insbesondere für Auftragsverarbeitung nach Art. 28 DSGVO
- ausländische Dienstleister nach Art. 45 ff. DSGVO eingebunden
- datenschutzrechtliche Regelungen/Pflichten werden an Subunternehmer weitergegeben
- formalisierte Auftragserteilung (Auftragsformulare)
- die mit der Auftragserfüllung betrauten Personen und Dienstleister kennen die Weisungen aus dem Vertrag und sind datenschutzrechtlich unterwiesen
- Kontrolle der Vertragsausführung
- regelmäßige Kontrolle der Dienstleister, insbesondere toMs. Alle 2 Jahre auf Dokumentenbasis prüfen lassen (Dienstleister anschreiben, toM Prüfung ankündigen. Dienstleister muss alle Unterlagen betreffend toMs zurückschicken.)
- dokumentierter Prozess bei Datenschutzvorfällen
- Datenschutzfolgenabschätzung bei Risikoprozessen

7. Verfügbarkeit, Datensicherung

Es ist zu gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind, insbesondere Maßnahmen zur Datensicherung (physikalisch / logisch).
Der Auftragnehmer ist nicht verpflichtet vom Auftraggeber gelöschte Daten wiederherzustellen

- Brandschutzmaßnahmen im Serverraum und Büros
- Überspannungsschutz
- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage
- RAID-Verfahren, Spiegeln von Festplatten
- Einsatz eines Ausweich-RZ
- Backupkonzept (täglich, wöchentlich, monatlich)
- getrennte Aufbewahrung/Speicherung der Datensicherung
- Virenschutzkonzept
- Standardverfahren/Patchmanagement zur regelmäßigen Aktualisierung von Schutzsoftware (z.B. Virenscanner)
- dokumentiertes Notfallkonzept

- Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung

8. Belastbarkeit

Es ist zu gewährleisten, dass IT-Systeme widerstandsfähig sind, insbesondere gegen Hacker- und Überlastangriffe wirksam geschützt werden können.

Maßnahmen zur Belastbarkeit:

- Virenschutz / Firewall
- Penetrationstests
- Verschlüsselung
- Notfallplan
- Protokollierung, Auswertung

9. Pseudonymisierung/Anonymisierung

Es ist zu gewährleisten, dass personenbezogene Daten bei Bedarf pseudonymisiert bzw. anonymisiert werden können.

Maßnahmen zur Pseudonymisierung/ Anonymisierung:

- bei Bedarf werden personenbezogene Identifikationsmerkmale wie Name, E-Mail-Adresse, IP-Adresse aus dem Datensatz entfernt
- die personenbezogenen Identifikationsmerkmale werden getrennt vorgehalten, um eine Repersonalisierung zu ermöglichen (Pseudonymisierung), oder werden endgültig gelöscht (Anonymisierung).

10. Trennungsgebot, Mandantenfähigkeit

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt werden, insbesondere Maßnahmen zur getrennten Verarbeitung von Daten mit unterschiedlichen Zwecken

- Mandantentrennung, Mandantenfähigkeit der Systeme
- Einhaltung der Zweckbindung
- getrennte Ordnerstrukturen (Auftragsdatenverarbeitung)
- Berechtigungskonzept, das die getrennte Verarbeitung von Kundendaten ermöglicht
- Funktionstrennung (Produktion, Testumgebung)