Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

-Verantwortlicher-

Unternehmen: _____

Name: _____

Straße: _____

PLZ/ Ort: _____

(im folgenden - **Auftraggeber** - genannt)

und dem

- Auftragsverarbeiter-

Unternehmen: Martin Becker GmbH
Straße: Birkenallee 135
PLZ/ Ort: 48432 Rheine

(im folgenden - **Auftragnehmer** - genannt)

schließen zur Leistungsvereinbarung (Hauptvertrag) laut jeweils aktuell geltender Auftragsgrundlage (z.B. Auftrag laut Angebot, Kostenübernahme, Dauer-Kostenübernahme, Service-Vereinbarung) nachfolgenden Vertrag über die Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer:

Präambel:

Diese Vereinbarung zur Auftragsverarbeitung (AV) ergänzt jede vertragliche Vereinbarung (einschl. aller zugehörigen bzw. entsprechenden Dokumente wie Leistungsbeschreibungen, SaaS, Anhänge, Anlagen, etc.) zwischen dem Auftraggeber und dem Auftragnehmer oder dem Auftraggeber und mit dem Auftragnehmer verbundene Unternehmen über den Bezug von Leistungen und Produkten, soweit der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers oder mit dem Auftraggeber verbundene Unternehmen verarbeitet (Hauptvertrag).

Sie gilt für alle mit dem jeweilig entstandenen Hauptvertrag in Verbindung stehenden Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder vom Auftragnehmer beauftragte Dritte personenbezogene Daten im Auftrag des Auftraggebers verarbeiten. Diese AV beinhaltet in Verbindung mit dem Hauptvertrag die dokumentierten Weisungen für die Verarbeitung personenbezogener Daten, Gegenstand, Dauer, Konkretisierung des Auftragsinhalts, Art und Zweck der Verarbeitung, sowie die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung von jeweils per Auftrag laut Angebot / Kostenübernahme / Dauer-Kostenübernahme / Service-Vereinbarung geregelten Aufgaben durch den Auftragnehmer. Die Aufgaben richten sich nach Auftragsbestandteil und enthalten meist:

- ✓ Installation/Einrichtung/Anpassung/Schulung von Hotelsoftware- und Kassen-Systemen nach Hersteller-Standard und Vorgabe des Auftraggebers
- ✓ Technische Installation und Inbetriebnahme von Hardware- und Netzwerk-Komponenten nach Hersteller-Standard und Vorgabe des Auftraggebers
- ✓ Einrichtung eines Netzwerks unter Berücksichtigung der Wünsche und Vorgaben des Auftraggebers

(2) Dauer

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages. Sollten Leistungen auch noch nach Beendigung des Hauptvertrages erbracht werden, so gelten die Regelungen dieser Vereinbarung auch für diese weitere Leistungserbringung für die gesamte Dauer der tatsächlichen Kooperation fort.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung bzw. dem Hauptvertrag (Auftrag laut Angebot / Kostenübernahme / Dauer-Kostenübernahme / Service-Vereinbarung) konkretisiert.

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 wird vorher mit dem Auftraggeber abgestimmt und erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. erfüllt sind. Die Überprüfung der besonderen Voraussetzungen erfolgt seitens des Auftragnehmers.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- ✓ Personenstammdaten
- ✓ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ✓ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ✓ Vertragsabrechnungs- und Zahlungsdaten
- ✓ Planungs- und Steuerungsdaten
- ✓ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ✓ Bankverbindungsdaten
- ✓ Bestelldaten
- ✓ Adressdaten
- ✓ Kundenhistorie

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ✓ Kunden
- ✓ Interessenten
- ✓ Abonnenten
- ✓ Beschäftigte
- ✓ Lieferanten
- ✓ Handelsvertreter
- ✓ Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) 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.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 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].

(3) 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 werden dokumentiert.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) 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.

(2) 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 verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des Auftraggebers. Gemäß den Art. 28 bis 33 DS-GVO gewährleistet der Auftragnehmer hierbei die Einhaltung folgender Vorgaben:

(1) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 Abs. 1 DSGVO bestellt hat und wird diesen gegenüber dem Auftraggeber schriftlich oder in Textform (z.B. E-Mail) benennen.

(2) Der Auftragnehmer bestätigt, dass er bei der Durchführung der Arbeiten nur Beschäftigte einsetzt, die gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO 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.

(3) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
Die bezieht sich insbesondere auf:

- 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.

(4) Der Auftragnehmer sichert die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages zu.

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

6. 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 kann Unterauftragnehmer (weitere Auftragsverarbeiter) mit der Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers beauftragen.
Der Auftragnehmer hat dabei sicherzustellen, dass allen Unterauftragsnehmern, die personenbezogene Daten im Auftrag von im Europäischen Wirtschaftsraum ansässigen Kunden im Wege eines Vertrages oder eines anderen Rechtsinstruments nach dem Recht der EU oder eines EU-Mitgliedstaates verarbeiten, mindestens gleichwertige Datenschutzpflichten, wie die in dieser AV geregelten, auferlegt werden, wobei insbesondere hinreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen vorzusehen sind.

Die jeweiligen Unterauftragsnehmer des Auftragnehmers werden im Falle des Einsatzes separat gegenüber dem Auftraggeber genannt. Auf explizite Anfrage in schriftlicher Form stellt der Auftragnehmer eine Auflistung seiner entsprechenden Unterauftragnehmer schriftlich zur Verfügung.

Mindestens zwanzig (20) Kalendertage vor der Beauftragung oder eines Wechsels eines neuen Unterauftragsnehmers hat der Auftragnehmer seinen Auftraggeber entsprechend zu informieren. Der Auftraggeber ist berechtigt, der Beauftragung bzw. dem Einsatz eines neuen Unterauftragnehmers bei der Verarbeitung personenbezogener Daten in seinem Auftrag innerhalb einer Frist von zehn (10) Werktagen zu widersprechen. Der Widerspruch ist per Email an datenschutz@mb-gmbh.de zu richten, wobei der vollständige Name (und andere Daten zur eindeutigen Identifizierung) des Auftraggebers zu nennen sowie auf den entsprechenden Hauptvertrag Bezug zu nehmen und Gründe für den Widerspruch anzugeben sind. Übt der Auftraggeber sein Widerspruchsrecht aus, so hat der Auftragnehmer nach freiem Ermessen das Recht:

a) vom Einsatz des beanstandeten Unterauftragsnehmer bei der Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers abzusehen und dies dem Auftraggeber schriftlich zu bestätigen
b) den Auftraggeber zu kontaktieren, um eine einvernehmliche Einigung mit ihm zu suchen, z.B. durch Beseitigung des Grundes für den Widerspruch. Kommt zwischen den Parteien eine Vereinbarung zustande, nimmt der Auftraggeber den Widerspruch zurück.
c) den Hauptvertrag insgesamt oder nur hinsichtlich jener Verarbeitung im Auftrag des Auftraggebers zu kündigen, für welche der beanstandete neue Unterauftragsnehmer beauftragt werden soll.
d) Für jede Übermittlung personenbezogener Daten in ein Land außerhalb der EU, müssen die Voraussetzungen des Art. 44 DSGVO erfüllt sein.

(3) 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.

7. Kontrollrechte des Auftraggebers

(1) 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.

(2) 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.

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

8. Mitteilung bei Verstößen des Auftragnehmers

(1) 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.

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
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) 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
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) 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

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

(2) 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.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber, 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.

(3) 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. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Nebenabreden bedürfen der Schriftform.

(3) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen.
Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Ort, Datum:

_____

Unterschrift - **Auftraggeber** -

Ort, Datum: Rheine, 24.Mai 2018

Unterschrift - **Auftragnehmer** -
vertreten durch Martin Becker, Philipp Becker

Martin Becker GmbH
Birkenallee 135 • 48432 Rheine
Tel. 05971/80826 0 • Fax 05971/80826 26
www.mb-gmbh.de • info@mb-gmbh.de

Commerzbank Rheine
BIC: COBADEFFXXX
IBAN: DE17403400300150202000
Stadtsparkasse Rheine
BIC: WELADED1RHN
IBAN: DE85403500050000037218

Geschäftsführer: Martin Becker, Philipp Becker
Amtsgericht Steinfurt HRB 4296
Umsatzsteuer-IdNr: DE 165475716
Steuernummer: 311/5810/0781

Anlage 1
Technisch-organisatorische Maßnahmen (TOM) der Martin Becker GmbH

Der Verantwortliche trifft nach Artikel 32 DSGVO nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit.

Vertraulichkeit der Systeme und Dienste

Zutrittskontrolle

1. Das Gebäude ist gegen Einbruch bzw. unbefugten Zugang bauseits gesichert.

2. Das Gebäude ist durch ein umfangreiches Gefahrenmeldesystem sowie eine nachgeschalteten externen Wachschutz über eine Gefahrenmeldezentrale gesichert.

3. Der Zugang zum Gebäude wird für Mitarbeiter durch ein mit Schließgruppen und Berechtigungen versehenes Schließsystem sichergestellt.

4. Der Gebäudezugang findet für Mitarbeiter und Dritte ausschließlich durch den zentralen und gesicherten Eingang mit Empfangsbereich statt.

5. Es existieren eine Zutrittsregelung sowie definierte Prozesse zur Vergabe von Zugangsberechtigungen an Mitarbeiter.

6. Dritte können sich im Gebäude auf der Basis von Regeln nur nach Anmeldung und in Begleitung eines Mitarbeiters bewegen.

7. Der Zugang zu besonders schützenswerten Räumen (u.a. Serverraum) sind mit zusätzlichen technischen und organisatorischen Schutzmaßnahmen versehen.

8. Zur Ergänzung der organisatorischen Maßnahmen gilt ein Vier-Augen-Prinzip für alle Mitarbeiter.

Zugangskontrolle

1. Der Zugang zu Daten und Systemen erfolgt auf Basis eines Berechtigungssystems mit Benutzerprofilen, Zuordnung der Profile zu genutzten IT-Systemen sowie einer Protokollierung. Eine Nutzung von IT-Systemen ist nur durch Identifikation mit Account-/Benutzername und Passwort möglich.

2. Ein zyklischer Passwortwechsel ist im Rahmen einer Passwortrichtlinie geregelt.

3. Es existiert eine differenzierte Zugriffregelung auf der Basis von Benutzerprofilen.

4. Als zusätzliche Maßnahme werden separate virtuelle Server-Instanzen zur Trennung von Systemen, Projekten und Kommunikation eingesetzt.

5. Es existieren definierte Prozesse zur Vergabe und Entzug von Zugangsberechtigungen.

6. Es existieren Richtlinien für die Bezeichnung und Ablage von Daten.

7. Eine Ablage von Dateien darf ausschließlich nur auf verifizierten Endgeräten und Speichermedien erfolgen.

8. Als Schutz von Server- und Clients wird eine Virensoftware mit aktuellen Signaturen verwendet.

9. Zum Schutz externer Zugänge auf Server und Clients wird eine softwarebasierte Firewall eingesetzt.

Zugriffskontrolle

1. Der Zugriff auf Daten und Systeme ist durch Benutzerprofile differenziert und jeweils eingeschränkt. Eine Anmeldung ist immer erforderlich.

2. Der Zugriff auf Daten erfolgt über ein geregeltes, profilbasiertes Berechtigungssystem.

3. Der Zugriff auf Daten und Systeme wird protokolliert.

4. Zur Vernichtung von vertraulichen und personenbezogenen Papierdaten erfolgt die Aktenvernichtung über einen externen Dienstleister, welcher Aktenvernichter mind. der Klasse 2 einsetzt.

5. Datenträger (u.a. Festplatten) werden nach Maßgabe des Standes der Technik gelöscht und anschließend physisch zerstört.

6. Das Speichern von Daten ist durch eine Richtlinie nur auf Netzlaufwerken und verifizierten mobilen Datenträgern erlaubt.

7. Der Zugriff sowie die Änderung von personenbezogenen Daten wird in den entsprechenden Systemen protokolliert. Änderungen dieser Daten ist nur einem definierten Benutzerkries im Rahmen von Richtlinien möglich.

Pseudonymisierung und Verschlüsselung personenbezogener Daten

1. Eine aktuelle Verschlüsselung wird für die WLAN-Nutzung eingesetzt.

2. Geschäfts- und Personaldaten werden gesondert gespeichert und verschlüsselt.

3. Es werden externe durch VPN-Zugänge für dedizierte Aufgaben auf Basis aktueller Zertifizierungs- und Verschlüsselungstechnologien nur für definierte Benutzer bereitgestellt.

4. Es wird Datenverschlüsselung für alle Medien eingesetzt (Server, Clients, Datenträger, Dateien, etc.).

5. Es erfolgt eine bedarfsorientierte Verschlüsselung insbesondere von Daten, die übertragen werden oder sich auf mobilen Geräten befinden. Sensible Daten (u.a. personenbezogene Daten), die elektronisch (z.B. per Email) übermittelt werden müssen, werden grundsätzlich verschlüsselt.

6. Personendaten, die auf der Webseite des Unternehmens erfasst werden, werden verschlüsselt übertragen.

Integrität der Systeme und Dienste

Eingabekontrolle

1. Die Änderung von personenbezogenen Daten erfolgt auf der Basis von definierten Berechtigungen sowie organisatorischen Regelungen.

2. Der Zugriff sowie die Änderung von personenbezogenen Daten wird in den entsprechenden Systemen protokolliert. Änderungen dieser Daten ist nur einem definierten Benutzerkries im Rahmen von Richtlinien möglich.

Weitergabekontrolle

1. Es werden grundsätzlich keine personenbezogenen Daten aktiv an Dritte ohne rechtliche Grundlage weitergegeben.

2. Ausgesonderte Datenträger werden nachhaltig physisch vernichtet.

3. Ein externer Zugang für definierte Mitarbeiter ist als VPN-Tunnel mit nur eingeschränktem Zugriff möglich.

4. Der Umgang mit Datenträgern sowie die Verschlüsselung von Daten, die übergeben werden ist in einer Richtlinie vorgegeben.

Trennung von Daten

1. Für alle genutzten Systeme und durchgeführte Projekte existiert eine physikalisch oder logisch getrennte Datenhaltung (Mandantentrennung).

2. Für die getrennten Daten existieren jeweils eigene Berechtigungsgruppen, die funktionsabhängig und personenbezogen zugewiesen werden (Funktionstrennung).

3. Für die Entwicklung von Software existiert eine Trennung von Produktions- und Testsystemen.

Verfügbarkeit und Belastbarkeit der Systeme und Dienste

1. Gebäude und Serverraum sind mit Messeinrichtungen zur Identifikation von Gefahren durch z.B. Brand, Rauch ausgestattet.

2. Die Verfügbarkeit wird durch Virtualisierung von Servern und kontinuierlichem Backup sichergestellt. Datensicherungen werden nach dem 3-2-1 an mehreren Standorten angelegt.

3. Der Serverraum ist mit Feuerlöscher und entsprechenden Schutzsteckdosen für die Server sowie USV ausgestattet.

4. Die Überwachung der Verfügbarkeit der zentralen Systeme erfolgt durch automatisierte Softwaremeldungen.

Wiederherstellung der Verfügbarkeit der personenbezogenen Daten nach Zwischenfall

1. Eine vollständige Wiederherstellung aller Systeme wird innerhalb von 24 Stunden durch Notfallpläne angestrebt.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Es sind Richtlinien für IT-Sicherheit und Datenschutz vorhanden (u.a. Passwortrichtlinie, Speicherung von Daten, Umgang mit Datenträgern, etc.)

2. Beschäftigte sind entweder nach §5 BDSG oder werden nach Artikel 5 DSGVO zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet. Sofern Dritte zu genehmigten und beaufsichtigten Wartungszwecken einen Zugang zu personenbezogenen Daten haben könnten, wird sichergestellt, dass diese durch den Auftragnehmer zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet sind.

3. Beschäftigte werden bzgl. des Umgangs mit personenbezogenen Daten und Maßnahmen zum Datenschutz vertraut gemacht.

4. Ein externer Datenschutzbeauftragter wurde benannt.

5. Es gibt ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO.

6. Es gibt definierte Datenschutzverfahren

7. Eine Auswahl von Dienstleistern erfolgt sorgfältig und durch Prüfung, Dokumentation, Vereinbarung und Kontrolle bzgl. der Einhaltung des gültigen Datenschutzgesetzes und der Datensicherheit für personenbezogene Daten. Sofern eine Auftragsverarbeitung vorliegt erfolgt der Abschluss eines entsprechenden Auftragsverarbeitungsvertrages.

Martin Becker GmbH
Birkenallee 135 • 48432 Rheine
Tel. 05971/80826 0 • Fax 05971/80826 26
www.mb-gmbh.de • info@mb-gmbh.de

Commerzbank Rheine
BIC: COBADEFFXXX
IBAN: DE17403400300150202000
Stadtsparkasse Rheine
BIC: WELADED1RHN
IBAN: DE85403500050000037218

Geschäftsführer: Martin Becker, Philipp Becker
Amtsgericht Steinfurt HRB 4296
Umsatzsteuer-IdNr: DE 165475716
Steuernummer: 311/5810/0781