

Minkenberg Medien GmbH · Roermonder Str. 128 a · 52525 Heinsberg

Vertrag MMTOMS

Version 0.1.070518-std

Datenschutzbeauftragter

Roman Nowack

zert. Datenschutzbeauftragter (IHK)

zert. Datenschutzauditor (TÜV)

EU-CON BeraterForum GmbH

Technisch-organisatorische Maßnahmen des Auftragnehmers

Firma GmbH Minkenberg Medien GmbH
Str., Nr. Roermonder Straße 128a
PLZ, Ort 52525 Heinsberg
(nachfolgend „Auftragnehmer“ / „Auftragsverarbeiter“)

dokumentiert und bereitgestellt für

Firma GmbH _____
Str., Nr. _____
PLZ, Ort _____
(nachfolgend „Auftraggeber“ / „Verantwortlicher“)

1. Zutrittskontrolle

A.	Serverseitig getroffene Zutrittskontrollmaßnahmen
1.0	Werden die Auftragsdaten des Auftraggebers auf von Ihnen oder in Ihrem Auftrag betriebenen Servern physikalisch gespeichert? ☒ ja ☐ nein
Wenn 1.0 nein: In diesem Fall müssen Sie die Fragen 1.1 bis 1.29 <u>nicht beantworten</u>. Bitte gehen Sie dann gleich zu Frage 1.30 über! Auch die Fragen 7.1 bis 7.20. entfallen.	
1.1	Nennen Sie die Standorte des Serverraums und der Rechenzentrums (RZ). ☒ Minkenberg Medien GmbH, Roermonder Straße 128a, 52525 Heinsberg
	Sind die Auftragsdaten auf mehr als einen Serverstandort / Rechenzentrum verteilt (z. B. Backup Server/ Nutzung von Cloud-Dienstleistungen)? ☒ ja ☐ nein
1.3	Falls 1.2 ja: Machen Sie bitte die entsprechenden Adressangaben auch bzgl. weiterer Server. Weitere Serverstandort: vgl. 1.1
1.4	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für alle im Einsatz befindlichen Server- / RZ Standorte? ☒ ja ☐ nein
1.5	Falls 1.4 nein: Beantworten Sie bitte die Fragen 1.6 bis 1.29 und 7.1 bis 7.20 für weitere RZ- / Serverstandorte.
1.6	Wird der Server / das RZ durch Sie (AN) selbst, oder durch einen Dienstleister / Subunternehmer betrieben? ☒ Auftragnehmer ☐ Dienstleister
1.7	Sofern der Server durch einen Subunternehmer betrieben wird, nennen Sie bitte Namen und Sitz des Dienstleisters Klicken Sie hier, um Text einzugeben.
1.8	Im wievielten Stock steht der Server, auf dem die Auftragsdaten gespeichert werden?

	☒ EG ☐ Keller bitte Geschoßzahl eintragen OG
1.9	Ist der Serverraum fensterlos? ☒ ja ☐ nein
1.10	Wenn 1.9 nein: Wie sind die Fenster vor Einbruch geschützt? ☐ vergittert ☐ alarmgesichert ☐ abschließbar ☐ gar nicht ☐ Sonstiges: bitte eintragen
1.11	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja ☒ nein
1.12	Wenn 1.11 ja: Wer wird informiert, wenn die EMA auslöst? Mehrfachantworten möglich! ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
1.13	Ist der Serverraum mit einem elektronischen Schließsystem versehen? ☐ ja ☒ nein
1.14	Wenn 1.13 ja: Welche Zutrittstechnik kommt zum Einsatz? Mehrfachantworten möglich! ☐ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges: persönliche Kontrolle
1.15	Wenn 1.13 ja: Sind die Zutrittstechniken personenbezogen vergeben / personifiziert? ☐ ja ☐ nein
1.16	Wenn 1.13 ja: Werden die Zutritte zum Raum im Zutrittssystem gespeichert/protokolliert? ☐ ja, sowohl erfolgreiche / positive, als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche / positive Zutritte ☐ nein, das Schloss wird nur freigegeben oder nicht
1.17	Wenn 1.16 ja: Wie lange werden die Zutrittsdaten ungefähr gespeichert? - / - Tage

1.18	Existiert ein mechanisches Schloss? ☒ ja ☐ nein
1.19	Wenn 1.18 ja , wie viele Schlüssel zum Serverraum existieren und wo werden diese aufbewahrt. Anzahl Schlüssel: 1 Aufbewahrungsort: Rezeption
1.20	Wenn 1.18 ja : Wird die Schlüsselausgabe protokolliert? ☐ ja ☒ nein
1.21	Wenn 1.18 ja : Wie wird protokolliert und wer gibt die Schlüssel aus? ☐ Schlüsselbuch Ausgabestelle: Geschäftsleitung
1.22	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Anzahl der Personen: 3 Funktion im Unternehmen: Büroorganisation, Administration
1.23	Ist der Serverraum videoüberwacht? ☐ ja ☒ nein
1.24	Wenn 1.23 ja : Wie lange werden die Bilddaten gespeichert? - / - Tage
1.25	Wie ist der Zutritt durch betriebsfremde Personen zum Serverraum geregelt? (bspw. Im Falle von Wartungsdiensten / Elektrikern / Reinigungspersonal). ☐ es gibt keine Regelung ☒ Zutritt & Anwesenheit nur in Begleitung ☐ Sonstiges: bitte eintragen
1.26	Werden Zutritte durch Betriebsfremde zum Serverraum protokolliert? ☐ ja ☒ nein
1.27	Aus welchem Material besteht die Zugangstür zum Serverraum? ☐ Stahl / Metall ☒ sonstiges Material
1.28	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt? ☒ ja ☐ nein

1.29 **Wenn 1.28 ja:** Was wird in dem Serverraum noch aufbewahrt?

- ☐ Telefonanlage ☒ Lagerung Büromaterial ☐ Lagerung Akten ☐ Archiv
- ☐ Lagerung von IT Ausstattung ☐ Sonstiges: bitte eintragen

B.	Clientseitig getroffene Zutrittskontrollmaßnahmen
1.30	Nennen Sie bitte die genaue Adresse des Standorts der Clientarbeitsplätze, von denen auf die Auftragsdaten zugegriffen wird. Minkenberg Medien GmbH, Roermonder Straße 128a, 52525 Heinsberg
1.31	Ist das Bürogebäude vollständig umfriedet (Zaun, Mauer o.ä.). ☐ ja ☒ nein
1.32	Im wievielten Stock befinden sich die Büroräume? ☒ EG ☐ Keller ☒ im gesamten Gebäude Nur im Geschoßzahl eintragen OG
1.33	Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros? ☒ ja ☐ nein
1.34	Wird ein Besucherbuch geführt? ☒ ja ☐ nein
1.35	Ist das Gebäude / die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja ☒ nein
1.36	Wenn 1.35 ja: Wer wird informiert, wenn die EMA auslöst? ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
1.37	Ist das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen? ☐ ja, Gebäude und Büroräume sind elektronisch verschlossen ☐ ja, aber nur das Gebäude, nicht der Eingang zu den Büros / zur Büroetage. ☐ ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt. ☒ nein
1.38	Wenn ja 1.37: Welche Zutrittstechnik kommt zum Einsatz? Mehrfachantworten möglich!

	☐ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges: Schlüssel
1.39	Wenn 1.37 ja: Sind die Zutrittstechniken personenbezogen vergeben / personifiziert? ☐ ja ☐ nein
1.40	Wenn 1.37 ja: Werden die Zutritte im Zutrittssystem gespeichert/protokolliert? ☐ ja, sowohl erfolgreiche / positive, als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche / positive Zutritte ☐ nein, das Schloss wird nur freigegeben oder nicht.
1.41	Wenn 1.37 ja: Wie lange werden die Zutrittsdaten ungefähr gespeichert? bitte Wert in Tagen eintragen Tage
1.42	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? ☒ ja ☐ nein
1.43	Wird die Ausgabe von Schlüsseln protokolliert und wer gibt die Schlüssel aus? ☐ nein, die Ausgabe wird nicht protokolliert ☒ ja, die Ausgabe wird mittels eines Formulars / Schlüsselbuch dokumentiert. Ausgabestelle ist: Geschäftsleitung
1.44	Ist das Bürogebäude, bzw. seine Zugänge videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☒ nein

1.45	Wenn 1.44 „ja, mit Bildaufzeichnung“, wie lange werden die Bilddaten gespeichert? bitte Wert in Tagen eintragen Tage
1.46	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen? ☐ nein ☒ ja, betriebsfremde Personen werden am Eingang / Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.

2. Zugangskontrolle

2.1	Existiert ein persönlicher Passwort / (PW) Benutzername Zugangsschutz zu den Systemen, mit denen die Auftragsdaten verarbeitet werden? ☒ ja ☐ nein
2.2	Wie werden die Zugangsberechtigungen vergeben? ☒ auf Antrag (schriftlich oder Mail) an IT ☒ Antrag muss durch Vorgesetzten genehmigt sein ☐ Sonstige Vergabeweise: bitte angeben
2.3	Existiert für die Administration der Systeme ein eigenständiger ADMIN-Account, der sich von seinem eigentlichen User-Account des Admins unterscheidet? ☒ ja ☐ nein, der Admin benutzt die Systeme immer als angemeldeter ADMIN
2.4	Existieren verbindliche Passwortparameter im Unternehmen? ☒ ja ☐ nein
2.5	Wie lauten die Passwort (PW) Vorgaben: PW Länge: ☒ 8 Zeichen oder mehr ☐ Weniger als 8 Zeichen ☐ Weniger als 6 Zeichen Welche Zeichenarten müssen erfüllt sein? ☒ Sonderzeichen ☒ Ziffern ☒ Groß- / Kleinschreibung Gültigkeitsdauer des PW: ☒ 90 Tage oder weniger ☐ 180 Tage oder weniger ☐ mehr als 180 Tage
2.6	Nach wie vielen Zyklen darf ein Nutzer dasselbe PW frühestens erneut vergeben (Passworthistorie)? ☐ keine Vorgabe ☒ 1 - 2 Zyklen ☐ 3 – 5 Zyklen ☐ mehr als 5 Zyklen
2.7	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben?

	☒ ja ☐ nein
2.8	Ist eine automatische PW geschützte Bildschirmsperre eingestellt? ☒ ja ☐ nein
2.9	Wenn 2.8 ja , Nach wie vielen Minuten der Inaktivität aktiviert sich die Bildschirmsperre? 3 Minuten
2.10	Existieren verbindliche Vorgaben zum manuellen Sperren des Clients beim Verlassen des Arbeitsplatzes? ☒ ja, der Rechner ist manuell zu sperren ☐ nein
2.11	Kontrollieren Sie die Aktualität der Zugangsberechtigungen? ☐ ja, regelmäßig ☒ nein, nur im Falle eines konkreten Anlasses
2.12	Welche Maßnahmen ergreifen Sie bei Verlust / Vergessen / Ausspähen eines PW? ☒ Admin setzt neues PW, das der Nutzer dann nach Erstanmeldung zu ändern hat ☐ keine

2.13	Gibt es eine Begrenzung von Anmeldeversuchen mit einem Benutzernamen / PW? ☒ ja ☐ nein
2.14	Wenn 2.13 ja, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgreicher Anmeldeversuche erreicht worden ist? ☒ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre durch die IT gesperrt ☐ Die Zugänge bleiben für bitte Wert in Minuteneintragen Minuteneinen gewissen Zeitraum gesperrt.
2.15	Bei Fernzugängen (VPN / IPSec): Mehrfachantworten möglich! Authentisierung mit ☒ pre-shared key ☐ Zertifikat PW Länge: ☒ 8 Zeichen oder mehr ☐ Weniger als 8 Zeichen ☐ Weniger als 6 Zeichen Welche Zeichenarten müssen erfüllt sein? ☐ Sonderzeichen ☒ Ziffern ☒ Groß- / Kleinschreibung Gültigkeitsdauer des PW: ☐ 90 Tage oder weniger ☐ 180 Tage oder weniger ☒ mehr als 180 Tage
2.16	Gibt es eine Begrenzung von Anmeldeversuchen bei Fernzugängen? ☒ ja ☐ nein
2.17	Wenn 2.16 ja, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgreicher Anmeldeversuche erreicht worden ist? ☒ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre durch die IT gesperrt ☐ Die Zugänge bleiben für bitte Wert in Minuteneintragen Minuten gesperrt.
2.18	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? ☒ ja ☐ nein

2.19	Wie viele MA haben über Fernzugänge Zugang auf die Daten des AG? 1 Personen. Läuft der Zugang über die Fernzugänge über ☐ Sammelkennung ☒ individuelle Einzelkennung?
2.20	Werden die Systeme, auf denen die Daten des Auftraggebers verarbeitet werden, über eine Firewall abgesichert? ☒ ja ☐ nein
2.21	Wenn 2.20 ja: Wird die Firewall regelmäßig upgedatet? ☒ ja ☐ nein
2.22	Wenn 2.20 ja: Wer administriert Ihre Firewall? ☒ eigene IT ☐ Externer Dienstleister
2.23	Wenn ein externer DL zum Einsatz kommt: Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten? ☐ ja ☐ nein, die Aufschaltung ist nur im 4 Augenprinzip mit einem Mitarbeiter der eigenen IT möglich.
2.24	Wenn ein externer DL zum Einsatz kommt: Haben Sie einen Vertrag zur Auftragsdatenverarbeitung mit diesem abgeschlossen? ☐ ja ☐ nein

3. Zugriffskontrolle

3.1	Existiert ein differenzierendes Berechtigungskonzept, das den Zugriff Ihrer Mitarbeiter auf die Daten des Auftraggebers regelt? ☒ ja ☐ nein
3.2	Wie werden die Zugriffsberechtigungen Ihrer Mitarbeiter auf die Daten des Auftraggebers vergeben? Mehrfachantworten möglich! ☐ auf Antrag (schriftlich oder Mail) an IT ☒ Antrag muss durch Vorgesetzten genehmigt sein
3.3	Wie wird gewährleistet, dass die Zugriffsberechtigungen bei Abteilungs- / Funktionswechsel und / oder Ausscheiden eines Mitarbeiters aktualisiert / entzogen werden? Mehrfachantworten möglich! ☐ personelle Veränderungen werden der IT Abteilung durch die Personalabteilung gemeldet. ☐ die zuständigen Vorgesetzten haben personelle Änderungen in ihrer Abteilung an die IT zu melden. ☒ Die Berechtigungen werden nach Art der Änderungen / des Wechsels angepasst bzw. entzogen. ☐ Sonstiges: bitte angeben
3.4	Werden Vergabe / Änderungen von Zugriffsberechtigungen protokolliert? ☒ ja ☐ nein
3.5	Existieren getrennte Produktiv- und Testsysteme im Falle der Notwendigkeit der Wartung der Systeme? ☒ ja ☐ nein
3.6	Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten, CD-ROMs, DVDs / Disketten), auf denen Auftragsdaten gespeichert sind, in Ihrem Unternehmen entsorgt? ☐ Physikalische Zerstörung durch eigene IT. ☒ Physikalische Zerstörung durch externen Dienstleister.

	☐ Sonstiges: bitte angeben
3.7	Wie werden nicht mehr benötigte Unterlagen mit personenbezogenen Daten des Auftraggebers (bspw. Ausdrucke / Akten / Schriftwechsel) in Ihrem Unternehmen entsorgt? ☐ Altpapier / Restmüll ☒ Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist. ☐ Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden. ☐ Sonstiges: bitte angeben
3.8	Wenn bei Ziff. 3.7 ein externer DL zum Einsatz kommt: Haben Sie einen Vertrag zur Auftragsdatenverarbeitung mit diesem abgeschlossen? ☐ ja ☐ nein
3.9	Dürfen Ihre MA eigene Speichermedien (z.B. USB Sticks) verwenden? ☐ generell ja ☒ ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT. ☐ nein, alle benötigten Speichermedien werden vom Unternehmen gestellt.

4. Weitergabekontrolle

4.1	Wie erfolgt der Datentransfer zwischen Ihnen und dem AG? Mehrfachantworten sind möglich! ☒ Webportal ☐ mobiler Datenträger ☒ E-Mail (Text und Anhänge wie PDF- / Excel- / Worddateien) ☐ Fax ☐ Schriftlich ☒ telefonisch ☐ FTP Server ☐ Share Point ☒ Einsichtnahme am Monitor (bspw. Fernwartung per Teamviewer o.ä.) ☒ Sonstiges (z.B. Clouddienste wie Drop Box): eigener File Sharing Dienst
4.2	Wenn die Daten elektronisch übertragen werden, erfolgt dieser Transfer verschlüsselt / technisch geschützt? ☐ nein (z.B. http / FTP) ☐ nein, aber persönliche Übergabe (bspw. Ausdrucke, Speichermedien wie bspw. DVDs) ☒ ja, per PW geschütztem ZIP Archiv / PDF / Excel File als Mailanhang ☐ ja, per PGP ☐ ja, per verschlüsselten Datenträger ☐ ja, per verschlüsseltem VPN ☒ ja, per https / SSL ☐ ja, per SFTP ☐ ja, Sonstiges: bitte angeben
4.3	Gibt es eine Vereinbarung, welche Personen auf Seite des AG und des AN die Daten übertragen dürfen? ☒ ja ☐ nein
4.4	Wenn 4.3 ja: Wer ist jeweils zur Übertragung von Auftragsdaten befugt? Für den AN: Name & Funktion angeben Für den AG: Name & Funktion angeben
4.5	Werden die Übertragungsvorgänge protokolliert? ☒ ja ☐ nein
4.6	Werden Auftragsdaten des AG durch Ihr Unternehmen (bzw. Ihre Mitarbeiter) auch auf mobilen Endgeräten verarbeitet?

	☐ ja ☒ nein
4.7	Wenn 4.6 ja: Wie sind die Endgeräte bzw. die darauf gespeicherten Auftragsdaten bei der Übertragung gesichert? Mehrfachantworten sind möglich! ☐ außer dem Schutz durch die allgemeine PW / Benutzerkennung keine weiteren Maßnahmen. ☐ Verschlüsselung der Festplatten / Verzeichnisse gem. modernen Standards ☐ über eine VPN-Verbindung zum eigenen Firmennetz ☐ über eine VPN-Verbindung zum Auftraggeber ☐ Sonstiges: bitte angeben
4.8	Wenn 4.6 ja: Verarbeiten Ihre Mitarbeiter Auftragsdaten des AG auch auf eigenen privaten Geräten (bring your own device)? ☐ ja ☒ nein
4.9	Können Ihre Mitarbeiter auf die Daten des Auftraggebers vom Home Office aus zugreifen. ☒ ja ☐ nein

5. Eingabekontrolle

5.1	Werden Zugriffe (Lesen, Änderungen, Löschen) auf Daten des Auftraggebers personenbezogen protokolliert? ☒ ja ☐ nein
5.2	Wenn 5.1 ja: Wie lange werde diese Protokolldaten aufbewahrt? 365 Tage
5.3	Wenn 5.1 ja: ? Werden die Protokolle ausgewertet? ☐ ja ☒ nein, eine Auswertung wäre aber im Bedarfsfall möglich
5.4	Wenn 5.1 <u>nein</u>: Ist zumindest der letzte Zugriff auf die Daten (Uhrzeit / Datum der Änderung) feststellbar? ☒ ja ☐ nein

6. Auftragskontrolle

6.1	Hat Ihr Unternehmen schriftlich einen fachkundigen Datenschutzbeauftragten (DSB) bestellt? ☐ ja, interner DSB (Mitarbeiter des Auftragnehmers) ☒ ja, externer DSB ☐ nein
6.2	Wenn 6.1 ja: Nennen Sie bitten den Namen und Kontaktdaten Ihres DSB. Name: Roman Nowack, EU-CON BeraterForum GmbH Telefonnummer: +49 (0) 2452 - 99 33 12 E-Mail-Adresse: r.nowack@eu-con.net
6.3	Wenn 6.1 ja: Welche nachweisbare Qualifikation besitzt der bestellte DSB? ☐ keine ☒ nachweisbare Lehrgangsteilnahme zum Datenschutzbeauftragten (bspw. beim TÜV, IHK o.ä.)

	☐ es handelt sich um einen Juristen ☐ es handelt sich um einen Informatiker ☐ Sonstige Qualifikation: bitte angeben
6.4	Zu Ziff. 6.1 und 6.3: Bitte legen Sie die Bestellungsurkunde und den Fachkundenachweis in Kopie / als Scan dem AG zur Kontrolle vor. ☒ Kopie der Bestellungsurkunde wurde dem AG vorgelegt ☒ Kopie des Fachkundenachweis wurde dem AG vorgelegt
6.5	Werden Ihre MA, die Auftragsdaten verarbeiten, nachweislich im Datenschutzrecht geschult? ☒ ja, Präsenzschulungen ☐ ja, eLearning ☐ Merkblätter / Handouts ☐ nein
6.6	Werden Ihre MA schriftlich auf das Datengeheimnis verpflichtet? ☒ ja ☐ nein
6.7	Werden Ihre MA (soweit erforderlich) schriftlich auf das Sozialgeheimnis verpflichtet? ☐ ja ☐ nein
6.8	Setzen Sie zur Erfüllung Ihrer Pflichten aus dem Vertrag mit dem AG auch weitere Subunternehmer ein? ☒ ja ☐ nein
6.9	Sind die von Ihnen eingesetzten Subunternehmer dem AG gegenüber benannt worden und vom AG genehmigt? ☒ ja ☐ nein, bisher noch nicht
6.10	Wenn 6.9 nein: Nehmen Sie bitte umgehend mit dem AG Kontakt auf, um die Tätigkeit und Identität der bisher nicht genehmigten Subunternehmer zu klären.
6.11	Falls 6.8 ja: Wie stellen Sie sicher, dass Ihre Subunternehmer die Vorgaben dieses Vertrages mit dem AG und die Sie betreffenden Weisungen und Sicherheitsmaßnahmen umsetzen. Mehrfachantworten

	möglich!!! ☐ Kein Prozess hierzu vorhanden ☐ Die technisch-organisatorischen Sicherheitsmaßnahmen der Subunternehmer wurden bereits überprüft. Die Überprüfung wurde dokumentiert. Die Dokumentation wird dem AG auf Anfrage zur Verfügung gestellt. ☒ Die technisch-organisatorischen Sicherheitsmaßnahmen der Subunternehmer werden zeitnah überprüft. Die Überprüfung wird dokumentiert. Die Dokumentation wird dem AG anschließend zur Verfügung gestellt. ☐ Mit den Subunternehmern werden Verträge nach § 11 BDSG geschlossen. Diese können nach Aufforderung durch den AG vorgelegt werden. ☐ Eine Auftragskontrolle hat noch nicht stattgefunden.
6.12	Wurde Ihr Unternehmen bereits einmal von einer Aufsichtsbehörde für den Datenschutz überprüft oder zertifiziert? ☐ ja ☒ nein
6.13	Wenn 6.12 ja: Sind Sie in der Lage, die Dokumentation der Prüfung / Zertifizierung dem AG vorzulegen. ☐ ja ☐ nein

7. Verfügbarkeitskontrolle

A.	Serverseitig getroffene Verfügbarkeitskontrollmaßnahmen
7.1	Verfügt der Serverraum über eine feuerfeste / feuerhemmende Zugangstür (bspw. F 90)? ☒ ja ☐ nein
7.2	Ist der Serverraum mit Rauchmeldern ausgestattet? ☒ ja ☐ nein
7.3	Ist der Serverraum an eine Brandmeldezentrale angeschlossen? ☒ ja ☐ nein
7.4	Ist der Serverraum mit Löschsystemen ausgestattet? Mehrfachantworten möglich! ☐ ja, CO2 Löscher ☐ ja, Halon / Argon Löschanlage ☐ Sonstiges: bitte angeben
7.5	Woraus bestehen die Außenwände des Serverraumes? ☐ Massivwand (bspw. Beton, Mauer) ☐ Leichtbauweise
7.6	Ist der Serverraum klimatisiert? ☒ ja ☐ nein
7.7	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)? ☒ ja ☐ nein
7.8	Wird deren Funktionalität regelmäßig getestet? ☐ ja ☐ nein
7.9	Verfügt der Serverraum zusätzlich über ein Diesellaggregat? ☐ ja ☐ nein
7.10	Existiert in Ihrem Unternehmen ein dokumentiertes Backup Konzept?

	☒ ja ☐ nein
7.11	Wird die Funktionalität der Backup Wiederherstellung regelmäßig getestet? ☒ ja ☐ nein
7.12	Wenn 7.10 ja: Sind Sie in der Lage, dem AG auf Anforderung das Backup Konzept vorzulegen? ☒ ja ☐ nein
7.13	In welchen Rhythmus werden in Ihrem Unternehmen Backups der Systeme angefertigt, auf denen die Auftragsdaten gespeichert werden? ☐ Echtzeitspiegelung ☒ täglich ☐ ein bis dreimal pro Woche ☐ Sonstiges: bitte angeben
7.14	Auf was für Sicherungsmedien werden die Backups gespeichert? ☒ Zweiter redundanter Server ☐ Sicherungsbänder ☒ Festplatten ☐ Sonstiges: bitte angeben
7.15	Wo werden die Backups aufbewahrt / erstellt? ☒ Zweiter redundanter Server steht an einem anderen Ort ☐ Safe, feuerfest, dokumentensicher ☐ einfacher Safe ☐ Bankschließfach ☐ abgeschlossener Aktenschrank / Schreibtisch ☒ Im Serverraum ☒ Privathaushalt
7.16	Zu 7.15: Im Falle eines Transports der Backups: Wie wird dieser durchgeführt? ☐ Mitnahme durch einen MA der IT / Geschäftsleitung / Sekretärin ☐ Abholung durch Dritte (bspw. Bankmitarbeiter / Wachunternehmen) ☐ Sonstiges: bitte angeben

7.17	Sind die Daten der Sicherungen / Backups verschlüsselt? ☐ ja ☒ nein
7.18	Befindet sich der Aufbewahrungsort nach Ziff. 7.15 in einem vom primären Server aus betrachtet getrennten Brandabschnitt / Gebäudeteil? ☒ ja ☐ nein
B.	Allgemeine Verfügbarkeitskontrollmaßnahmen
7.19	Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisiertem ☒ Virenschutz ☒ Anti-Spyware ☒ Spamfilter ☒ Firewall
7.20	Existiert in Ihrem Unternehmen ein dokumentiertes Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)? ☐ ja ☒ nein

8. Trennungsgebot

8.1	Wie sind die Auftragsdaten des AG von anderen Daten(bspw. Daten des AN oder von anderen AG) getrennt? ☒ ja, logische Trennung ☐ ja, physische Trennung ☐ nein
8.2	Sind die zur Verarbeitung der Auftragsdaten eingesetzten Verfahren mandantenfähig? ☐ ja ☐ nein ☒ Es werden keine weiteren speziellen Verfahren eingesetzt, die Trennung erfolgt logisch auf Verzeichnisebene.

Heinsberg, den 15.05.2018

Ort & Datum



Unterschrift des Auftragnehmers

Hinweis:

Bei Änderungen der von Ihnen getroffenen und hier dokumentierten technischen – organisatorischen Sicherheitsmaßnahmen sind die Änderungen dem Auftraggeber unverzüglich mitzuteilen. Dieser Anhang ist dann entsprechend zu aktualisieren, mit dem aktuellen Tagesdatum zu versehen und durch Abstimmung mit dem Auftraggeber unter Ersetzung der Vorversion zum neuen Vertragsbestandteil zu machen.