

# Vertrag zur Auftragsverarbeitung personenbezogener Daten (gem. DSGVO) zwischen

**CleverReach GmbH & Co. KG**

Mühlenstr 43  
26180 Rastede

- nachstehend Auftragnehmerin genannt -

und

**MARGAYS e.V.**

**Kundennummer 32884**

Bahnhofstr. 27  
35037 Marburg, Deutschland

- nachstehend Auftraggeberin genannt -

## § 1 Gegenstand und Dauer des Auftrags

- (1) Die Auftragnehmerin führt die im Anhang 1 beschriebenen Dienstleistungen für die Auftraggeberin durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien werden dort beschrieben.
- (2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange die Auftragnehmerin für die Auftraggeberin personenbezogene Daten verarbeitet. Dieser Vertrag ersetzt gleichzeitig alle bisherigen Verträge zur Auftragsdatenverarbeitung zwischen den Vertragsparteien, sofern vorhanden.

## § 2 Weisungen der Auftraggeberin

- (1) Die Auftraggeberin ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.
- (2) Die Auftragnehmerin verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen der Auftraggeberin und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn die Auftraggeberin dies anweist. Die Auftragnehmerin darf hiervon abweichend in Ausnahmefällen die Daten, die sie im Auftrag der Auftraggeberin verarbeitet, berichtigen, löschen oder sperren, wenn sie aus rechtlichen Gründen dazu verpflichtet ist, E-Mail-Adressen aus der Datenbank zu entfernen und auf eine schwarze Liste zu setzen, wenn eine E-Mail an eine bestimmte und gleiche E-Mail-Adresse dreimal in Folge als unzustellbar zurückkommt (sog. Hardbounces) oder Beschwerden von Empfängern vorliegen.
- (3) Die Verarbeitung erfolgt nur auf Weisung der Auftraggeberin, es sei denn, die Auftragnehmerin ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem die Auftragnehmerin unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt die Auftragnehmerin der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

- (4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von der Auftraggeberin zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn die Auftragnehmerin dies verlangt.
- (5) Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Vorschriften verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen.

### **§ 3 Technische und organisatorische Maßnahmen**

- (1) Die Auftragnehmerin verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und im Anhang 3 dieses Vertrages zu dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
- (2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Die Auftragnehmerin darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss die Auftragnehmerin der Auftraggeberin nur wesentliche Anpassungen mitteilen.
- (3) Die Auftragnehmerin unterstützt die Auftraggeberin bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Die Auftragnehmerin hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten der Auftraggeberin mitzuwirken. Die Auftragnehmerin wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat der Auftraggeberin alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

### **§ 4 Pflichten der Auftragnehmerin**

- (1) Die Auftragnehmerin bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
- (2) Die Auftragnehmerin bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.
- (3) Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sie überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.
- (4) Die Auftragnehmerin darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten der Auftraggeberin zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.
- (5) Soweit gesetzlich vorgeschrieben, bestellt die Auftragnehmerin einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden der Auftraggeberin zum Zweck der direkten Kontaktaufnahme mitgeteilt.

- (6) Die Auftragnehmerin darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.
- (7) Die Auftragnehmerin unterstützt die Auftraggeberin mit geeigneten technischen und organisatorischen Maßnahmen, damit diese ihren bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Die Auftragnehmerin benennt einen Ansprechpartner, der die Auftraggeberin bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt der Auftraggeberin dessen Kontaktdaten unverzüglich mit. Soweit die Auftraggeberin besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt die Auftragnehmerin die Auftraggeberin hierbei. Auskünfte an die betroffene Person oder Dritte darf die Auftragnehmerin nur nach vorheriger Weisung der Auftraggeberin erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber der Auftragnehmerin geltend macht, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

## **§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen**

- (1) Die Auftragnehmerin darf Unterauftragnehmer nur beauftragen, wenn sie die Auftraggeberin immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch die Auftraggeberin die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen.
- (2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn die Auftragnehmerin weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen oder Reinigungskräfte. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
- (3) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn die Auftragnehmerin durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.
- (4) Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

## § 6 Kontrollrechte der Auftraggeberin

Die Auftragnehmerin erklärt sich damit einverstanden, dass die Auftraggeberin oder eine von ihr beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen oder durch Zutritt zu den Arbeitsräumen der Auftragnehmerin zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht der Auftragnehmerin zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

## § 7 Mitzuteilende Verstöße der Auftragnehmerin

Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten der Auftraggeberin mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten der Auftraggeberin. Gleiches gilt, wenn die Auftragnehmerin feststellt, dass die bei ihr getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Der Auftragnehmerin ist bekannt, dass die Auftraggeberin verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird die Auftragnehmerin die Auftraggeberin bei der Einhaltung ihrer Meldepflichten unterstützen. Sie wird die Verletzungen der Auftraggeberin unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,
- b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
- c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
- d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

## § 8 Beendigung des Auftrags

- (1) Nach Abschluss der Auftragsverarbeitung hat die Auftragnehmerin alle personenbezogenen Daten nach Wahl der Auftraggeberin entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
- (2) Die Auftraggeberin kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn die Auftragnehmerin einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeberin aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

## § 9 Schlussbestimmungen

- (1) Sollte das Eigentum der Auftraggeberin bei der Auftragnehmerin durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmerin die Auftraggeberin unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände der Auftraggeberin ausgeschlossen.
- (2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was ab dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.
- (3) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.
- (4) Als Gerichtsstand vereinbaren die Parteien, sofern gesetzlich zulässig, den Firmensitz der Auftragnehmerin.

Ort, Datum

Marburg, 25.05.2018

---

Ort, Datum

Rastede, 24.05.2018

Unterschrift Auftraggeberin



---

Unterschrift Auftragnehmerin



---

Geschäftsführung

## Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

|   |  |
|---|--|
| Gegenstand der Verarbeitung   | Bereitstellung der CleverReach-Software für den E-Mail-Versand/-Auswertung durch die Auftraggeberin.   |
| Art und Zweck der Verarbeitung  | Erhebung, Speicherung, Nutzung und Übermittlung von Account-Daten der Auftraggeberin.<br><br>Speicherung und Übermittlung von Empfängerdaten zum Zweck der Zusendung/Auswertung von E-Mails.   |
| Art der personenbezogenen Daten   | Account-Daten der Auftraggeberin <ul style="list-style-type: none"> <li>- Ansprache</li> <li>- Vor- und Nachname</li> <li>- Firma, Rechnungsanschrift</li> </ul> Empfängerdaten (E-Mail-Adresse, Vor- und Zuname) <ul style="list-style-type: none"> <li>- E-Mail-Adresse</li> <li>- Vor- und Nachname</li> <li>- Anschrift</li> </ul> <ul style="list-style-type: none"> <li>- Personenstammdaten</li> <li>- Kommunikationsdaten</li> <li>- Protokolldaten</li> </ul> |
| Kategorien betroffener Personen   | <ul style="list-style-type: none"> <li>- Ansprechpartner/Handelnde der Auftraggeberin</li> <li>- Newsletter-Empfänger</li> <li>- Käufer und Interessenten</li> </ul> <ul style="list-style-type: none"> <li>- Kunden und Interessenten</li> <li>- Mitarbeiter und Lieferanten</li> </ul>   |
| Name und Kontaktdaten des Datenschutzbeauftragten der Auftraggeberin (sofern vorhanden) |  |
| Name und Kontaktdaten des Datenschutzbeauftragten der Auftragnehmerin                   | Dr. Uwe Schläger, datenschutz nord GmbH<br>datenschutz nord GmbH<br>Konsul-Smidt-Str. 88<br>28217 Bremen<br>Deutschland<br>Ansprechpartner: Conrad S. Conrad, Justiziar<br>E-Mail: <a href="mailto:cconrad@datenschutz-nord.de">cconrad@datenschutz-nord.de</a>  |

## Anhang 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

| <b>Unterauftragnehmer</b> (Name, Rechtsform, Sitz der Gesellschaft) | <b>Verarbeitungsstandort</b> | <b>Art der Dienstleistung</b>                  |
|---|------------------------------|--|
| PlusServer GmbH   | Deutschland                  | Versand der E-Mails                            |
| Amazon Web Services, Inc.   | Irland<br>Deutschland        | Speicherung und Verarbeitung der Auftragsdaten |
|   |                              |  |
|   |                              |  |

## Anhang 3: Technisch-organisatorische Maßnahmen bei der CleverReach GmbH & Co. KG

### A Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität (1.1 Standort 1)

|           |   |
|-----------|---|
| <b>1.</b> | <b>Zutrittskontrollmaßnahmen zu Serverräumen</b>  |
| 1.1       | Werden personenbezogene Daten auf Servern gespeichert, die von Ihnen betrieben werden?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 1.2       | Nennen Sie bitte die Standorte des Serverraums / Rechenzentrums (RZ).<br><b>Standort 1:</b> Deutschland - hier werden keine Auftragsdaten gespeichert<br><b>Standort 2:</b> Amazon Web Services LLC, Irland<br><b>Standort 3:</b> PlusServer GmbH, Deutschland<br><b>Standort 4:</b> Amazon Web Services LLC, Deutschland |
| 1.3       | Sind die personenbezogenen Daten auf mehr als einen Serverstandort / Rechenzentrum verteilt (z. B. Backup Server/ Nutzung von Cloud-Dienstleistungen)?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 1.4       | <b>Falls 1.3 ja: Machen Sie bitte die entsprechenden Standortangaben auch bzgl. weiterer Server.</b><br>Weitere Serverstandorte:                      Amazon Web Services LLC, Irland   |
| 1.5       | Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für <b>alle</b> im Einsatz befindlichen Server- / RZ Standorte?<br><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein, ausschließlich für Standort 1   |
| 1.6       | Ist der Serverraum fensterlos?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 1.7       | Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 1.8       | Wenn 1.7 ja: Wer wird informiert, wenn die EMA auslöst?<br><input checked="" type="checkbox"/> beauftragter Wachdienst <input checked="" type="checkbox"/> Administrator <input checked="" type="checkbox"/> Leiter IT <input checked="" type="checkbox"/> Sonstiges: Polizei   |
| 1.9       | Ist der Serverraum videoüberwacht?<br><input type="checkbox"/> ja, ohne Bildaufzeichnung <input type="checkbox"/> ja, mit Bildaufzeichnung <input checked="" type="checkbox"/> nein   |
| 1.10      | Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne?<br>Anzahl der Personen: 3<br>Funktion im Unternehmen: Administratoren, Leiter IT  |
| 1.11      | Ist der Serverraum mit einem elektronischen Schließsystem versehen?<br><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein, mit mechanischem Schloss   |
| 1.12      | Wie viele Schlüssel zum Serverraum existieren, wo werden diese aufbewahrt, wer gibt die Schlüssel aus?<br>Anzahl Schlüssel: 3   Aufbewahrungsort: Schlüsselschrank und externes Gebäude<br>Ausgabestelle: Administrator   |
| 1.13      | Aus welchem Material besteht die Zugangstür zum Serverraum?<br><input checked="" type="checkbox"/> Stahl / Metall <input type="checkbox"/> sonstiges Material   |



|   |  |
|---|--|
| 1.14  | <p>Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt?</p> <p><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein</p>  |
|   | <p><b>Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p><input checked="" type="checkbox"/> geeignet <input type="checkbox"/> begrenzt geeignet <input type="checkbox"/> ungeeignet</p> <p>Begründung: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.</p> |
| <b>2. Zutrittskontrollmaßnahmen zu Büroräumen</b> |  |
| 2.1   | <p>Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird:</p> <p>Arbeitsplätze der Mitarbeiter</p>   |
| 2.2   | <p>Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros?</p> <p><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein</p>   |
| 2.3   | <p>Wird ein Besucherbuch geführt?</p> <p><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein</p>  |
| 2.4   | <p>Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?</p> <p><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein</p>   |
| 2.5   | <p>Wer wird informiert, wenn die EMA auslöst?</p> <p><input checked="" type="checkbox"/> beauftragter Wachdienst <input checked="" type="checkbox"/> Administrator <input checked="" type="checkbox"/> Leiter IT <input checked="" type="checkbox"/> Sonstiges: Polizei</p>  |
| 2.6   | <p>Werden das Bürogebäude bzw. seine Zugänge videoüberwacht?</p> <p><input checked="" type="checkbox"/> ja, ohne Bildaufzeichnung <input type="checkbox"/> ja, mit Bildaufzeichnung <input type="checkbox"/> nein</p>  |
| 2.7   | <p>Ist das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen?</p> <p><input type="checkbox"/> ja, Gebäude und Büroräume sind elektronisch verschlossen</p> <p><input checked="" type="checkbox"/> ja, aber nur das Gebäude, nicht der Eingang zu den Büros bzw. zur Büroetage.</p> <p><input type="checkbox"/> ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt.</p> <p><input type="checkbox"/> nein</p>  |
| 2.8   | <p><b>Wenn 2.7 ja:</b> Welche Zutrittstechnik kommt zum Einsatz?</p> <p><input checked="" type="checkbox"/> RFID <input checked="" type="checkbox"/> PIN <input type="checkbox"/> Biometrie <input type="checkbox"/> Sonstiges:</p>  |
| 2.9   | <p><b>Wenn 2.7 ja:</b> Werden die Zutrittsrechte personalifiziert vergeben?</p> <p><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein</p>  |
| 2.10  | <p><b>Wenn 2.7 ja:</b> Werden die Zutritte im Zutrittssystem protokolliert?</p> <p><input checked="" type="checkbox"/> ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche</p> <p><input type="checkbox"/> ja, aber nur erfolgreiche positive Zutritte</p> <p><input type="checkbox"/> ja, aber nur erfolglose Zutrittsversuche</p> <p><input type="checkbox"/> nein, das Schloss wird nur freigegeben oder nicht</p>   |
| 2.11  | <p><b>Wenn 2.10 ja:</b> Wie lange werden diese Protokolldaten aufbewahrt?</p> <p>6 Monate</p>  |

|          |  |
|----------|--|
| 2.12     | <p><b>Wenn 2.10 ja:</b> Werden die Protokolle regelmäßig ausgewertet?</p> <input type="checkbox"/> ja <input checked="" type="checkbox"/> nein, eine Auswertung ist aber im Bedarfsfall möglich  |
| 2.13     | <p>Existiert ein mechanisches Schloss für die Gebäude / Büroräume?</p> <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 2.14     | <p><b>Wenn 2.13 ja:</b> Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus?</p> <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein      Ausgabestelle: Administration   |
| 2.15     | <p>Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen?</p> <input type="checkbox"/> nein<br><input checked="" type="checkbox"/> ja, betriebsfremde Personen werden am Eingang bzw. Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.  |
|          | <p><b>Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p> <input checked="" type="checkbox"/> geeignet                      <input type="checkbox"/> begrenzt geeignet                      <input type="checkbox"/> ungeeignet         </p> <p>Begründung: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.</p> |
| <b>3</b> | <b>Zugangs- und Zugriffskontrollmaßnahmen</b>  |
| 3.1      | <p>Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen?</p> <input checked="" type="checkbox"/> definierter Freigabeprozess<br><input type="checkbox"/> kein definierter Freigabeprozess, auf Zuruf<br><input type="checkbox"/> sonstige Vergabeweise:  |
| 3.2      | <p>Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert?</p> <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein   |
| 3.3      | <p>Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst?</p> <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 3.4      | <p>Existieren verbindliche Passwortparameter im Unternehmen?</p> <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 3.5      | <p>Wie lauten die Passwort-Vorgaben für Zugriff auf auftragsdatenbezogene Zugriffe?</p> <p><b>PW Länge:</b><br/> <input checked="" type="checkbox"/> 10 Zeichen oder mehr    <input type="checkbox"/> Weniger als 8 Zeichen    <input type="checkbox"/> Weniger als 6 Zeichen         </p> <p><b>Welche Zeichenarten müssen erfüllt sein?</b><br/> <input type="checkbox"/> Sonderzeichen    <input checked="" type="checkbox"/> Ziffern    <input checked="" type="checkbox"/> Groß- / Kleinschreibung         </p> <p><b>Gültigkeitsdauer des PW:</b><br/> <input type="checkbox"/> 90 Tage oder weniger    <input type="checkbox"/> 180 Tage oder weniger    <input checked="" type="checkbox"/> mehr als 180 Tage         </p>   |

|      |   |
|------|---|
| 3.6  | Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 3.7  | Wird der Bildschirm bei Inaktivität des Benutzers gesperrt?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein<br>Wenn ja, nach wie vielen Minuten? Nach 10 Minuten  |
| 3.8  | Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts?<br><input checked="" type="checkbox"/> Admin vergibt neues Initialpasswort<br><input type="checkbox"/> keine  |
| 3.9  | Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen?<br><input checked="" type="checkbox"/> ja, nach 3 Versuchen <input type="checkbox"/> nein   |
| 3.10 | <b>Wenn 3.9 ja</b> , Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde?<br><input type="checkbox"/> Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt<br><input checked="" type="checkbox"/> Die Zugänge bleiben für 10 Minuten gesperrt.   |
| 3.11 | Wie erfolgt die Authentisierung bei Fernzugängen:<br>Authentisierung mit <input type="checkbox"/> Token <input checked="" type="checkbox"/> VPN-Zertifikat <input type="checkbox"/> Passwort  |
| 3.12 | Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen?<br><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein, ohne Zertifikat ist eine Anmeldeversuch nicht möglich   |
| 3.13 | Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt?<br><input checked="" type="checkbox"/> ja, nach 30 Minuten <input type="checkbox"/> nein   |
| 3.14 | Werden die Systeme über eine Firewall abgesichert?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 3.15 | <b>Wenn 3.14 ja</b> : Wird die Firewall regelmäßig upgedatet?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein   |
| 3.16 | <b>Wenn 3.14 ja</b> : Wer administriert Ihre Firewall?<br><input checked="" type="checkbox"/> eigene IT <input type="checkbox"/> Externer Dienstleister   |
|      | <b>Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b><br><input checked="" type="checkbox"/> geeignet <input type="checkbox"/> begrenzt geeignet <input type="checkbox"/> ungeeignet<br>Begründung: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. |

|  |  |
|--|--|
| <b>4</b>   | <b>Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und mobilen Endgeräten</b>  |
| 4.1  | <p>Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrücke / Akten / Schriftwechsel) entsorgt?</p> <p><input type="checkbox"/> Altpapier / Restmüll</p> <p><input checked="" type="checkbox"/> Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist.</p> <p><input checked="" type="checkbox"/> Auftragsdaten der Auftraggeber liegen nicht in Papierform vor.</p> |
| 4.2  | <p>Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt?</p> <p><input checked="" type="checkbox"/> Physikalische Zerstörung durch eigene IT.</p> <p><input type="checkbox"/> Physikalische Zerstörung durch externen Dienstleister.</p> <p><input type="checkbox"/> Löschen der Daten</p>   |
| 4.3  | <p>Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks)</p> <p><input checked="" type="checkbox"/> ja, aber ausschließlich von der Auftragnehmerin gestellte Datenträger</p> <p><input type="checkbox"/> nein</p>   |
| 4.4  | <p>Dürfen die Mitarbeiter private Datenträger (z.B. USB Sticks) verwenden?</p> <p><input type="checkbox"/> generell ja</p> <p><input type="checkbox"/> ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT.</p> <p><input checked="" type="checkbox"/> nein, alle benötigten Speichermedien werden von der Auftragnehmerin gestellt.</p>  |
| 4.5  | <p>Werden Auftragsdaten der Auftraggeberin durch die Mitarbeiter auch auf mobilen Endgeräten verarbeitet?</p> <p><input checked="" type="checkbox"/> ja, aber nur auf Weisung der Auftraggeberin und auf Geräten der Auftragnehmerin</p> <p><input type="checkbox"/> nein</p>  |
| 4.6  | <p>Verarbeiten Mitarbeiter personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)?</p> <p><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein</p>   |
| <p><b>Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p><input checked="" type="checkbox"/> geeignet <input type="checkbox"/> begrenzt geeignet <input type="checkbox"/> ungeeignet</p> <p>Begründung: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.</p> |  |

| 5   | Maßnahmen zur sicheren Datenübertragung  |
|-----|--|
| 5.1 | <p>Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt?</p> <p><input type="checkbox"/> gar nicht</p> <p><input type="checkbox"/> nein, Datenübertragung erfolgt per MPLS</p> <p><input type="checkbox"/> per verschlüsselter Datei als Mailanhang</p> <p><input type="checkbox"/> per PGP/SMime</p> <p><input type="checkbox"/> per verschlüsseltem Datenträger</p> <p><input type="checkbox"/> per VPN</p> <p><input checked="" type="checkbox"/> per SSL/TLS</p> <p><input checked="" type="checkbox"/> per SFTP</p> <p><input type="checkbox"/> Sonstiges:</p>  |
| 5.2 | <p>Wer verwaltet die Schlüssel bzw. die Zertifikate?</p> <p><input type="checkbox"/> Anwender selbst    <input checked="" type="checkbox"/> eigene IT    <input type="checkbox"/> Externer Dienstleister</p>   |
| 5.2 | <p>Werden die Übertragungsvorgänge protokolliert?</p> <p><input checked="" type="checkbox"/> ja    <input type="checkbox"/> nein</p>   |
| 5.3 | <p><b>Wenn 5.2 ja:</b> Wie lange werden diese Protokolldaten aufbewahrt?</p> <p>Dauerhaft</p>  |
| 5.4 | <p><b>Wenn 5.2 ja:</b> Werden die Protokolle regelmäßig ausgewertet?</p> <p><input type="checkbox"/> ja    <input checked="" type="checkbox"/> nein, eine Auswertung ist aber im Bedarfsfall möglich</p>   |
|     | <p><b>Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p><input checked="" type="checkbox"/> geeignet                      <input type="checkbox"/> begrenzt geeignet                      <input type="checkbox"/> ungeeignet</p> <p>Begründung: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.</p> |

## B. Maßnahmen zur Sicherstellung der Verfügbarkeit (A 1.1 Standort 1)

| 1.  | Serverraum   |
|-----|--|
| 1.1 | Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Zugangstür?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein   |
| 1.2 | Ist der Serverraum mit Rauchmeldern ausgestattet?<br><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein  |
| 1.3 | Ist der Serverraum an eine Brandmeldezentrale angeschlossen?<br><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein   |
| 1.4 | Ist der Serverraum mit Löschsystemen ausgestattet?<br><input checked="" type="checkbox"/> ja, CO2 Löscher <input type="checkbox"/> ja, Halon / Argon Löschanlage <input type="checkbox"/> Nein   |
| 1.5 | Woraus bestehen die Außenwände des Serverraumes?<br><input checked="" type="checkbox"/> Massivwand (bspw. Beton, Mauer) <input type="checkbox"/> Leichtbauweise <input type="checkbox"/> Brandschutzwand (bspw. F90)   |
| 1.6 | Ist der Serverraum klimatisiert?<br><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein   |
| 1.7 | Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 1.8 | Wird die Stromversorgung des Serverraums zusätzlich über ein Dieselaggregat abgesichert?<br><input type="checkbox"/> ja <input checked="" type="checkbox"/> nein   |
| 1.9 | Werden die Funktionalität 1.2, 1.3, 1.4, 1.7 und 1.8 regelmäßig getestet?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
|     | <p><b>Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p><input checked="" type="checkbox"/> geeignet <input type="checkbox"/> begrenzt geeignet <input type="checkbox"/> ungeeignet</p> <p>Begründung: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.</p> |
| 2   | Backup- und Notfall-Konzept, Virenschutz   |
| 2.1 | Existiert ein Backupkonzept?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein   |
| 2.2 | Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |

|      |  |
|------|--|
| 2.3  | <p>In welchem Rhythmus werden Backups vom Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden?</p> <p><input checked="" type="checkbox"/> Echtzeitspiegelung   <input checked="" type="checkbox"/> täglich   <input type="checkbox"/> ein bis dreimal pro Woche</p>  |
| 2.4  | <p>Auf was für Sicherungsmedien werden die Backups gespeichert?</p> <p><input checked="" type="checkbox"/> Zweiter redundanter Server   <input type="checkbox"/> Sicherungsbänder   <input type="checkbox"/> Festplatten</p>   |
| 2.5  | <p>Wo werden die Backups aufbewahrt?</p> <p><input checked="" type="checkbox"/> Zweiter redundanter Server steht an einem anderen Ort</p> <p><input type="checkbox"/> Safe, feuerfest, datenträger- und dokumentensicher</p> <p><input type="checkbox"/> abgeschlossener Aktenschrank / Schreibtisch</p> <p><input type="checkbox"/> Im Serverraum</p>   |
| 2.6  | <p>Sind die Backups verschlüsselt?</p> <p><input checked="" type="checkbox"/> ja   <input type="checkbox"/> nein</p>   |
| 2.7  | <p>Befindet sich der Aufbewahrungsort der Backups in einem vom primären Server aus betrachtet getrennten Brandabschnitt bzw. Gebäudeteil?</p> <p><input checked="" type="checkbox"/> ja   <input type="checkbox"/> nein</p>  |
| 2.8  | <p>Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement?</p> <p><input checked="" type="checkbox"/> ja   <input type="checkbox"/> nein   <input type="checkbox"/> Prozess existiert, ist jedoch nicht dokumentiert</p>  |
| 2.9  | <p><b>Wenn 2.8 ja</b>, wer ist für das Software- bzw. Patchmanagement verantwortlich?</p> <p><input type="checkbox"/> Anwender selbst   <input checked="" type="checkbox"/> eigene IT   <input type="checkbox"/> Externer Dienstleister</p>  |
| 2.10 | <p>Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)?</p> <p><input checked="" type="checkbox"/> ja   <input type="checkbox"/> nein</p>  |
| 2.11 | <p>Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisiertem</p> <p><input checked="" type="checkbox"/> Virenschutz   <input checked="" type="checkbox"/> Anti-Spyware   <input checked="" type="checkbox"/> Spamfilter   <input checked="" type="checkbox"/> Firewall   <input checked="" type="checkbox"/> Backup</p>   |
| 2.12 | <p><b>Wenn 2.11 ja</b>, wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter verantwortlich?</p> <p><input type="checkbox"/> Anwender selbst   <input checked="" type="checkbox"/> eigene IT   <input type="checkbox"/> Externer Dienstleister</p>   |
|      | <p><b>Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p><input checked="" type="checkbox"/> geeignet   <input type="checkbox"/> begrenzt geeignet   <input type="checkbox"/> ungeeignet</p> <p>Begründung: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.</p> |

| 3   | Netzanbindung  |
|-----|--|
| 3.1 | Verfügt das Unternehmen über eine redundante Internetanbindung?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein  |
| 3.2 | Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden?<br><input checked="" type="checkbox"/> ja <input type="checkbox"/> nein   |
| 3.3 | Wer ist für die Netzanbindung des Unternehmens verantwortlich?<br><input checked="" type="checkbox"/> eigene IT <input type="checkbox"/> Externer Dienstleister  |
|     | <p><b>Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p> <input checked="" type="checkbox"/> geeignet                                <input type="checkbox"/> begrenzt geeignet                                <input type="checkbox"/> ungeeignet         </p> <p>Begründung: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.</p> |