Vertrag zur Auftragsverarbeitung personenbezogener Daten
(gem. DSGVO)

zwischen

Human Networks GmbH
Im Alten Grund 2
36100 Petersberg

- nachstehend Auftragnehmer genannt -

und

Ihr Unternehmen mit Anschrift

-nachstehend Auftraggeber genannt -

§ 1 Gegenstand und Dauer des Auftrags

1. Der Auftragnehmer führt die im Anhang 1 beschriebenen Dienstleistungen für die Auftraggeber 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 der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet. Dieser Vertrag ersetzt gleichzeitig alle bisherigen Verträge zur Auftragsdatenverarbeitung zwischen den Vertragsparteien, sofern vorhanden. Er ist als Ergänzung der Buchung des Cloud-Dienstes Cleverworks für den Fall, das der Auftraggeber personenbezogene Daten im Cloud-Dienst Cleverworks verwaltet, abschließbar.

§ 2 Weisungen des Auftraggeber

1. Der Auftraggeber 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. Der Auftragnehmer verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen des Auftraggeber und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Auftraggeber dies anweist. Der Auftragnehmer darf hiervon abweichend in Ausnahmefällen die Daten, die er im Auftrag des Auftraggeber verarbeitet, berichtigen, löschen oder sperren, wenn er 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 ein 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 des Auftraggeber, es sei denn, der Auftragnehmer ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber 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 vom Auftraggeber zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftragnehmer dies verlangt.

5. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggeber gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

1. Der Auftragnehmer 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. Der Auftragnehmer darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau er bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss der Auftragnehmer dem Auftraggeber nur wesentliche Anpassungen mitteilen.

3. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Der Auftragnehmer hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten des Auftraggeber mitzuwirken. Der Auftragnehmer wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. der vorherigen Konsultation der Aufsichtsbehörden mit. Er hat dem Auftraggeber alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen. Die dadurch dem Auftragnehmer entstehenden Kosten übernimmt der Auftraggeber.

§ 4 Pflichten des Auftragnehmer

1. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

2. Der Auftragnehmer 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. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und das die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

4. Der Auftragnehmer darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten des Auftraggeber zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

5. Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

6. Der Auftragnehmer darf die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union oder Europäischen Wirtschaftsraum (EWR) verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggeber und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

7. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Personen erfüllen kann, z.B. die Information und Auskunft an die betroffenen Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung der das Recht auf Datenübertragbarkeit und Widerspruch.

   Der Auftragnehmer stellt dem Auftraggeber diese Funktion über den beauftragten Cleverworks Cloud-Dienst zur Verfügung. Um diese Funktion gesetzkonform einzusetzen, kann der Auftraggeber gegen Kostenübernahme eine individuelle Einweisung erhalten.

   Soweit der Auftraggeber besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt der Auftragnehmer den Auftraggeber hierbei. Auskünfte an die betroffene Person oder Dritte darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggeber erteilen.

   Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Etwaig dadurch dem Auftragnehmer entstehende Kosten trägt der Auftraggeber.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

1. Der Auftragnehmer darf Unterauftragnehmer nur beauftragen, wenn er den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die

Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen.

2. Ein Unterauftragsverhältnis liegt insbesondere vor, wenn der Auftragnehmer 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 der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggeber 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 der Auftragnehmer 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 des Auftraggeber

Die Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder eine von ihm 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 des Auftragnehmer zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. 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 des Auftragnehmer zur Dokumentation der Sicherheitsmaßnahmen im Sinne des §3 dieser Vereinbarung. Die Kontrollmaßnahmen begleitet der Auftragnehmer. Die daraus dem Auftragnehmer entstehenden Kosten trägt der Auftraggeber.

§ 7 Mitzuteilende Verstöße des Auftragnehmer

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggeber mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Auftraggeber. Gleiches gilt, wenn der Auftragnehmer feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Dem

Auftragnehmer ist bekannt, dass der Auftraggeber 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 der Auftragnehmer den Auftraggeber bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen des Auftraggeber 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 der Auftragnehmer alle personenbezogenen Daten des Auftraggeber entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

2. Der Auftraggeber kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeber aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

3. Der Vertrag endet zeitgleich, wenn der abgeschlossene Hauptvertrag für die Nutzung des Cloud-Dienstes Cleverworks beendet ist

§ 9 Schlussbestimmungen

1. Sollte das Eigentum des Auftraggeber 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 verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Auftraggeber ausgeschlossen.

2. Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was seit 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 des Auftragnehmer.

Ort, Datum	Ort, Datum
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anhang 1: Auflistung der beauftragten Dienstleistung mit Ansprechpartner für den Datenschutz

Gegenstand der Verarbeitung	Bereitstellung der Cleverworks-SAAS-Lösung für Email, SMS, Slack, Twitter-Versand und Auswertung durch den Auftraggeber selbst
Art und Zweck der Verarbeitung	Erhebung, Speicherung, Nutzung und Übermittlung von Zugangsdaten, Anschrift, Kommunikationsdaten und Ansprechpartner des Auftraggeber für Zugang und Rechnungsstellung. Zugangsprotokollierung. Speicherdauer gemäß gesetzlicher Vorschriften und gemäß internem Verfahrensverzeichnis Speicherung, Übermittlung und Auswertungsdaten von Kontaktdaten, verwaltet vom Auftraggeber selbst. Speicherdauer verwaltet der Auftraggeber selbst
Art und Kategorie der personenbezogenen Daten	Zur Erfüllung des Dienstes sowie gesetzlicher Anforderungen durch uns selbst vom Auftraggeber: Geschäftsanschrift für Rechnungsstellung nebst Kommunikationsdaten, Zugangsdaten mit verschlüsselter Passwort-Ablage, Zugangsprotokollierung mit IP-Adresse und Zeitstempel sowie anonymisierte Verhaltensdaten der verwalteten Kontakte zu statistischen Zwecken. Zugangsdaten zu Fremdsystemen, die der Auftraggeber selbst eingibt und von der Cleverworks-SAAS-Lösung für die Aussendung von Informationen an die Kontakte des Auftraggebers, gesteuert durch den Auftraggeber selbst, z.B. Email-Server-Daten, SLACK-Zugangsdaten, Twitter-Account-Daten Seitens des Auftraggebers: Jegliche Daten, die er selbst in das System übermittelt, speichert und nutzt. Und die Daten, die das System durch das Verhalten der Kontakte des Auftraggebers durch Aussendungen über die verfügbaren Kommunikationskanäle erhält. Der Auftragnehmer hat darauf keinen Einfluss
Name und Kontaktdaten des für den Datenschutz beauftragten des Auftragnehmers	Dipl. Inform. Thomas Schmitt Human Networks GmbH Im Alten Grund 2 36100 Petersberg Email: datenschutz@cleverworks.de

Anhang 2: Liste der von uns beauftragten Unterauftragnehmer

Unterauftragnehmer	Standort	Art der Dienstleistung
Hetzner Online GmbH	Deutschland	Bereitstellung der SAAS-Lösung Cleverworks einschließlich Datenablage der vom Auftraggeber gespeicherten Daten sowie verschlüsseltes Backup des Software-Kerns
Vautron Rechenzentrum AG	Deutschland	Bereitstellung der der SAAS-Lösung Cleverworks einschließlich Datenablage der vom Auftraggeber gespeicherten Daten sowie verschlüsseltes Backup des Software-Kerns
Verne Global	Island (EWR)	Geplanter Zusatz-Standort ab 2020 (auch für außereuropäische Auftraggeber) für Bereitstellung der SAAS-Lösung Cleverworks einschließlich Datenablage der vom Auftraggeber gespeicherten Daten sowie verschlüsseltes Backup des Software-Kerns

Anhang 3: Technisch-organisatorische Maßnahmen

1.	Zutrittskontrollmaßnahmen zu Serverräumen
	Werden personenbezogene Daten auf Servern gespeichert, die von Ihnen betrieben werden? Ja, sofern der Auftraggeber diese selbst abspeichert
	Sind die personenbezogenen Daten auf mehrere Standorte/Rechenzentren verteilt? Ja. Die Liste der Standorte entspricht der Liste der Unterauftragnehmer aus Anhang 2. Europäische Auftraggeber können sich schriftlich (per Email an datenschutz@cleverworks.de) gegen den Standort Verne Global aussprechen.
	Sind die Serverräume an allen Standorten mittels Einbruchmeldeanlage (EMA) alarmgesteuert? Ja.
	Wer wird informiert, wenn die EMA auslöst? Der beauftragte Wachdienst, der Administrator, der Leiter IT
	Sind die Serverräume videoüberwacht? Nein
	Welche Rollen der Mitarbeiter haben Zugang zu den Serverräumen Administratoren, IT-Leiter
	Aus welchem Material bestehen die Zugangstüren zu den Serverräumen? Aus Stahl/Metall
	Werden die Serverräume neben seiner eigentlichen Funktion anderweitig genutzt? Nein
	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? Ja, die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
2.	Zutrittskontrollmaßnahmen zu Büroräumen
	Standort der Mitarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: Arbeitsplätze der Mitarbeiter im Büro des Auftragnehmers, alternativ über Telearbeitsplätze autorisierter, besonders verpflichteter Mitarbeiter über Datenschutz-Telearbeitsregelungen
	Existiert ein ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros? Nein
	Wird ein Besucherbuch geführt Nein
	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? Ja
	Wer wird informiert, wenn die EMA auslöst? Der Leiter IT und der Geschäftsführer
	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht? Nein
	Ist das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen? Nein
	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? Ja. Die Herausgabe eines Schlüssels erfolgt seitens des Geschäftsführers und wird protokolliert
	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen?

	Ja, betriebsfremde Personen werden am Eingang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.
	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? Ja, die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
3	Zugangs- und Zugriffskontrollmaßnahmen
	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen? Ja
	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert? Ja
	Existieren verbindliche Passwortparameter im Unternehmen? Ja, eine zwingende Vorgabe mit 10 Zeichen oder mehr mit Ziffern, Sonderzeichen und einer Gültigkeitsdauer von mehr als 180 Tagen
	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? Ja, nach 5-10 Minuten
	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts? Der Administrator vergibt ein neues Initialpasswort, was er selbst nicht einsehen kann
	Wie erfolgt die Authentisierung bei Fernzugängen: Über VPN-Zertifikat
	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? Nein, ohne Zertifikat ist ein Anmeldeversuch verwehrt
	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? Ja, nach 15 Minuten
	Werden die Systeme über eine Firewall abgesichert und regelmäßig udgedated? Ja
	Wer administriert die eigene Firewall? Die eigene IT-Abteilung
	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? Ja, die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
4	Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und mobilen Endgeräten
	Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke / Akten / Schriftwechsel) entsorgt? Ja, hierfür stehen Schredder zur Verfügung, deren Nutzung angewiesen ist
	Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt? Ja, durch physikalische Zerstörung durch die IT-Abteilung
	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks) Ja, aber nur für Software, ohne darauf persönliche Daten abzulegen
	Dürfen die Mitarbeiter private Datenträger (z.B. USB Sticks) verwenden?

	Nein
	Werden Auftragsdaten des Auftraggeber durch die Mitarbeiter auch auf mobilen Endgeräten verarbeitet? Ja, aber nur dann, wenn dies auf Weisung des Auftraggeber erfolgt
	Verarbeiten Mitarbeiter personenbezogene Daten des Auftraggeber auch auf eigenen privaten Geräten (bring your own device)? Nein
	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? Ja, die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
5	Maßnahmen zur sicheren Datenübertragung
	Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt? Ja, per SSL/TLS/SFTP
	Wer verwaltet die Schlüssel bzw. die Zertifikate? Die IT-Abteilung
	Werden die Übertragungsvorgänge protokolliert? Ja, dauerhaft
	Werden die Protokolle regelmäßig ausgewertet? Nein, aber im Bedarfsfall möglich
	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? Ja, die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
6	Maßnahmen zur Sicherstellung der Verfügbarkeit
	Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Zugangstür? Ja
	Ist der Serverraum mit Rauchmeldern ausgestattet? Ja
	Ist der Serverraum mit Löschsystemen ausgestattet? Ja
	Woraus bestehen die Außenwände des Serverraumes? Aus einer Massivwand
	Ist der Serverraum klimatisiert? Ja
	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)? Ja
	Werden die Funktionalität Rauchmelder, Löschsystem, USV regelmäßig getestet? Ja
	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? Ja, die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
	Existiert ein Backupkonzept? Ja
	Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet? Ja
	In welchem Rhythmus werden Backups vom Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden? Ein bis dreimal pro Woche
	Auf was für Sicherungsmedien werden die Backups gespeichert? Backup-Server
	Wo werden die Backups aufbewahrt? Backup-Server an einem anderen Standort
	Sind die Backups verschlüsselt? Ja
	Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement? Ja, verantwortet durch die IT-Abteilung
	Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)? Ja
	Sind die IT Systeme technisch vor Datenverlusten und unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisierter Firewall und Backup, verantwortet durch die IT-Abteilung
	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? Ja, die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
7	Sonstige Maßnahmen
	Verfügt das Unternehmen über eine redundante Internetanbindung? Ja
	Wer ist für die Netzanbindung des Unternehmens verantwortlich? Der jeweilige Rechenzentrumsbetreiber, siehe Anhang 2
	Existieren Notfall- oder Recovery-Konzepte und Maßnahmen, die die Fähigkeit gewährleisten, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen? Ja
	Existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung? Ja
	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? Ja, die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.