Auftragsverarbeitung personenbezogener Daten

Version 2.4.1 vom 09.12.2020

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Kunde und Auftragnehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Kundes verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer übernimmt typischerweise folgende Verarbeitungen:

1. Managed Hosting: Einrichtung, Betrieb und Wartung von Webservern
2. Application Service Providing: Bereitstellen von Anwendungen auf den Servern
3. Support und Wartung: Eingriffe bei Störungen des Regelbetriebs, Pflege der Softwareinstallationen und des Betriebsystems
4. Erstellung und Versand von Marketingsendungen / Werbung auf den Webservern
5. Datenmanagement: Import / Export der Kontaktlisten von Interessenten, Teilnehmern, Kontakten
6. Analyse und Reporting: Auswertung aufgezeichneter Daten zum Gewinnen von Erkenntnissen

Die konkreten Verarbeitungen werden vom Auftragnehmer laufend im Verarbeitungsverzeichnis dokumentiert, das dem Kunden jederzeit zur Einsicht zur Verfügung steht.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag (im Folgenden „Hauptvertrag“).

2.2 Dauer

Die Verarbeitung beginnt mit dem Abschluss des Hauptvertrags und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1 Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Abgleich oder Verknüpfung, Einschränkung.

Die Verarbeitung dient folgenden Zwecken:

- Werbung für eigene und fremde Produkte und Diensteistungen
- Analyse der Werbewirksamkeit und des Website-Verkehrs

3.2 Art der Daten

Es werden folgende Daten verarbeitet:

- Kontaktdaten von Interessenten, Kunden
- Bewegungsdaten (besuchte URLs, abgesendete Formulare, heruntergeladene Dateien, versendete Emails)

3.2.1 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Website-Besucher
- Interessenten
- Mitarbeiter des Kunden
- Mitarbeiter des Auftragnehmers

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Kunde angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Kundem vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Kunden bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Kunden auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Kunde durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Kunden im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Kunden erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Kunden weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In

Zweifelsfällen kann sich der Kunde direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Kunden unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Kunden unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Kunden und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

(11) Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Kunden unverzüglich mitzuteilen.

5 Technische und organisatorische Maßnahmen

(1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Kunden unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Kunden nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Kunden unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Kunden nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Die Verarbeitung von Daten in Privatwohnungen ist nur mit vorheriger schriftlicher Zustimmung des Kunden im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Kunden uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

(7) Dedizierte Datenträger, die vom Kunden stammen bzw. für den Kunden genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

(8) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Kunde spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Kunden berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Kunden wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Kundes im Einzelfall zugelassen.

(2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Kunde erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

(3) Ausgenommen von der Pflicht zur Einholung der Zustimmung des Kunden ist der Einsatz von freien Mitarbeitern. Für diese wird abweichend von den vorstehenden Regelungen ein Recht auf Ablehnung des Einsatzes für den Kunden vereinbart. Macht der Kunde von diesem Recht Gebrauch, ist der Auftragnehmer verpflichtet, den freien Mitarbeiter nicht mehr einzusetzen und einen weiteren Zugriff auf die verarbeiteten Daten zu unterbinden.

(4) Die Rechte des Kundeen müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Kunde berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(5) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(6) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

(7) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(8) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat.

(9) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrags genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Kunden mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

(10) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Kunde unaufgefordert vorzulegen.

(11) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Kunden.

(12) Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Kunden genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(13) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen, Webhosting, Domain-Providing oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8 Rechte und Pflichten des Kundes

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Kunde verantwortlich.

(2) Der Kunde erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Kunde unverzüglich dokumentiert bestätigen.

(3) Der Kunde informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Kunde ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Kunden zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Kunden Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Kunden benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Kunden unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Kunden bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Der Kunde behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Kunde und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Kunden unverzüglich darauf aufmerksam machen, wenn eine vom Kunden erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Kunden bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses - oder jederzeit auf Verlangen des Kunden - hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Kunden entweder zu vernichten oder an den Kunden zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 1.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Kunde unverzüglich vorzulegen.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Kunden bei Vertragsende übergeben.

12 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Kunde und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Kunden auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Kunden erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Kunden ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der Auftragnehmer haftet gegenüber dem Kunden für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Kunden erteilten Weisung entstanden ist.

14 Sonderkündigungsrecht

(1) Der Kunde kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Kundes nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Kunden vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Kunde dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Kunde zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

(4) Der Auftragnehmer hat dem Kunden alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrags oder dieses Vertrags in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.

15 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrags vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Kundes beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Kunden unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. §273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

-- Ende der Vertragsbestimmungen --

Anlage 1 – Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1 Dokumentation der Implementierung

Die folgende Tabelle gibt den Stand der umgesetzten technischen und organisatorischen Maßnahmen wieder (Stand 01.12.2020).

A Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.	**Zutrittskontrollmaßnahmen zu Serverräumen**
1.0	Werden personenbezogene Daten auf Servern gespeichert, die von Ihnen betriebenen werden? (Auch Auftragsverarbeitung) ☒ ja ☐ nein
	Die folgenden Angaben beziehen sich auf die zugesicherten TOM der Provider / Subdienstleister. **Content Optimizer betreibt keine eigenen Server / Rechenzentren.**
1.1	Standort des Serverraums / Rechenzentrums (RZ). OVH GmbH, Frankfurt, Deutschland, Hetzner GmbH,Nürnberg, Deutschland, Host Europe GmbH, Köln, Deutschland
1.2	Sind die personenbezogenen Daten 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 Standortangaben auch bzgl. weiterer Server.** Weitere Serverstandorte: Klicken Sie hier, um Text einzugeben.
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 1.21 und B für weitere RZ- / Serverstandorte.**
1.6	Ist der Serverraum fensterlos? ☒ ja ☐ nein

1.7	Wenn 1.6 nein: Wie sind die Fenster vor Einbruch geschützt? ☐ vergittert ☐ alarmgesichert ☐ abschließbar ☐ gar nicht ☐ Sonstiges: bitte eintragen
1.8	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☒ ja ☐ nein
1.9	Wenn 1.8 ja: Wer wird informiert, wenn die EMA auslöst? **Mehrfachantworten möglich!** ☒ beauftragter Wachdienst ☒ Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
1.10	Ist der Serverraum videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☒ ja, mit Bildaufzeichnung ☐ nein
1.11	**Wenn 1.10 ja, mit Bildaufzeichnung**: Wie lange werden die Bilddaten gespeichert? Unbekannt, interne Regelung des Providers
1.12	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Anzahl der Personen: Unbekannte Anzahl von Mitarbeitern der Provider Funktion im Unternehmen: Administratoren
1.13	Ist der Serverraum mit einem elektronischen Schließsystem versehen? ☒ ja ☐ nein, mit mechanischem Schloss
1.14	**Wenn 1.13 ja**: Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!** ☒ RFID ☐ PIN ☒ Biometrie ☒ Sonstiges: Vereinzelungsanlage
1.15	**Wenn 1.13 ja**: Werden die Zutrittsrechte personifiziert vergeben? ☒ ja ☐ nein
1.16	**Wenn 1.13 ja**: Werden die Zutritte zum Raum im Zutrittssystem protokolliert? ☒ ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche Zutritte ☐ ja, aber nur erfolglose Zutrittsversuche ☐ nein, das Schloss wird nur freigegeben oder nicht
1.17	**Wenn 1.16 ja**: Wie lange werden die Zutrittsdaten ungefähr gespeichert? Unbekannt, interne Regelung des Providers
1.18	**Wenn 1.13 nein**, wie viele Schlüssel zum Serverraum existieren, wo werden diese aufbewahrt, wer gibt die Schlüssel aus? Anzahl Schlüssel: Schlüsselanzahl Aufbewahrungsort: Aufbewahrungsort eintragen Ausgabestelle: bitte Ausgabestelle angeben
1.19	Aus welchem Material besteht die Zugangstür zum Serverraum? ☐ Stahl / Metall ☐ sonstiges Material
1.20	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt? ☐ ja ☒ nein
1.21	**Wenn 1.20 ja**: Was wird in dem Serverraum noch aufbewahrt? ☐ Telefonanlage ☐ Lagerung Büromaterial ☐ Lagerung Akten ☐ Archiv ☐ Lagerung von IT Ausstattung ☐ Sonstiges: bitte eintragen
2.	**Zutrittskontrollmaßnahmen zu Büroräumen**
2.1	Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: Essen, Deutschland
2.2	Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros?

	☐ ja ☒ nein
2.3	Wird ein Besucherbuch geführt? ☒ ja ☐ nein
2.4	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja ☒ nein
2.5	**Wenn 2.4 ja**: Wer wird informiert, wenn die EMA auslöst? ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ Sonstiges: bitte eintragen
2.6	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☒ nein
2.7	**Wenn 2.6 „ja, mit Bildaufzeichnung“,** wie lange werden die Bilddaten gespeichert? bitte Wert in Tagen eintragen Tage
2.8	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 bzw. zur Büroetage. ☐ ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt. ☒ nein
2.9	**Wenn 2.8 ja**: Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!** ☐ RFID ☐ PIN ☐ Biometrie ☒ Sonstiges: Schlüssel
2.10	**Wenn 2.8 ja**: Werden die Zutrittsrechte personifiziert vergeben? ☐ ja ☐ nein
2.11	**Wenn 2.8 ja**: Werden die Zutritte im Zutrittssystem protokolliert? ☐ ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche positive Zutritte ☐ ja, aber nur erfolglose Zutrittsversuche ☒ nein, das Schloss wird nur freigegeben oder nicht
2.12	**Wenn 2.11 ja**: Wie lange werden diese Protokolldaten aufbewahrt? bitte Wert in Tagen eintragen Tage
2.13	**Wenn 2.11 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☒ nein, eine Auswertung wäre aber im Bedarfsfall möglich
2.14	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? ☒ ja ☐ nein
2.15	**Wenn 2.14 ja**: Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus? ☒ ja ☐ nein Ausgabestelle: Geschäftsleitung
2.16	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen? ☐ nein ☒ ja, betriebsfremde Personen werden am Eingang bzw. Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.
3	**Zugangs- und Zugriffskontrollmaßnahmen**
3.1	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen? ☐ definierter Freigabeprozess

	☐ kein definierter Freigabeprozess, auf Zuruf ☒ Sonstige Vergabeweise: Abarbeitung einer Checkliste durch die Geschäftsführung.
3.2	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert? ☐ ja ☒ nein
3.2	Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst? ☐ ja ☒ nein
3.3	Existieren verbindliche Passwortparameter im Unternehmen? ☒ ja ☐ nein
3.4	**Passwort-Zeichenlänge:** 20 Zeichen, Alnum, Passwort-Manager mit YubiKey Token **Muss das Passwort Sonderzeichen enthalten?** ☒ ja ☐ nein **Mindest-Gültigkeitsdauer in Tagen:** keine
3.5	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben? ☒ ja ☐ nein
3.6	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? ☒ ja ☐ nein Wenn ja, nach wieviel Minuten? 5 Minuten
3.7	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts? ☒ Admin vergibt neues Initialpasswort ☐ keine
3.8	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen? ☒ ja, 5 Versuche ☐ nein
3.9	**Wenn 3.8 ja**, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde? ☒ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☐ Die Zugänge bleiben für bitte Wert in Minuteneintragen Minuten gesperrt.
3.10	Wie erfolgt die Authentisierung bei Fernzugängen: Authentisierung mit ☒ Token ☒ VPN-Zertifikat ☒ Passwort
3.11	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? ☒ ja, 5 ☐ nein
3.12	**Wenn 3.11 ja**, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☒ Die Zugänge bleiben für 1440 Minuten gesperrt.
3.13	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? ☐ ja, nach 10 Minuten ☒ nein
3.15	Werden die Systeme, auf denen personenbezogene Daten verarbeitet werden, über eine Firewall abgesichert? ☒ ja ☐ nein
3.16	**Wenn 3.15 ja:** Wird die Firewall regelmäßig upgedatet?

	☒ ja ☐ nein
3.17	**Wenn 3.15 ja**: Wer administriert Ihre Firewall? ☒ eigene IT ☐ Externer Dienstleister
3.18	**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.
4	**Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und mobilen Endgeräten**
4.1	Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke / Akten / Schriftwechsel) 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
4.2	Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt? ☒ Physikalische Zerstörung durch eigene IT. ☐ Physikalische Zerstörung durch externen Dienstleister. ☐ Löschen der Daten ☐ Löschen der Daten durch bitte Anzahl angeben Überschreibungen ☐ Sonstiges: bitte angeben
4.3	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks) ☒ ja ☐ nein
4.4	Dürfen die Mitarbeiter private Datenträger (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.
4.6	Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt? ☒ Verschlüsselung der Festplatte ☒ Verschlüsselung einzelner Verzeichnisse / Dateien ☐ keine Maßnahmen
4.7	Verarbeiten Mitarbeiter personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)? ☐ ja ☒ nein
5	**Maßnahmen zur sicheren Datenübertragung**
5.1	Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt? ☐ gar nicht ☐ nein, Datenübertragung erfolgt per mpls ☐ nur vereinzelt ☐ per verschlüsselter Datei als Mailanhang

	☐ per PGP/SMime ☐ per verschlüsseltem Datenträger ☒ per VPN ☒ per https/TLS ☒ per SFTP ☐ Sonstiges: bitte angeben
5.2	Wer verwaltet die Schlüssel bzw. die Zertifikate? ☒ Anwender selbst ☒ eigene IT ☐ Externer Dienstleister
5.2	Werden die Übertragungsvorgänge protokolliert? ☒ ja ☐ nein
5.3	**Wenn 5.2 ja**: Wie lange werden diese Protokolldaten aufbewahrt? 90 Tage
5.4	**Wenn 5.2 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☒ nein, eine Auswertung wäre aber im Bedarfsfall möglich

B. Maßnahmen zur Sicherstellung der Verfügbarkeit

1.	**Serveraum**
1.1	Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Zugangstür? ☒ ja ☐ nein
1.2	Ist der Serverraum mit Rauchmeldern ausgestattet? ☒ ja ☐ nein
1.3	Ist der Serverraum an eine Brandmeldezentrale angeschlossen? ☒ ja ☐ nein
1.4	Ist der Serverraum mit Löschsystemen ausgestattet? **Mehrfachantworten möglich!** ☐ ja, CO2 Löscher ☒ ja, Halon / Argon Löschanlage ☒ Sonstiges: Sauerstoffreduktion
1.5	Woraus bestehen die Außenwände des Serverraumes? ☒ Massivwand (bspw. Beton, Mauer) ☐ Leichtbauweise ☐ Brandschutzwand (bspw. F90)
1.6	Ist der Serverraum klimatisiert? ☒ ja ☐ nein
1.7	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)? ☒ ja ☐ nein
1.8	Wird die Stromversorgung des Serverraums zusätzlich über ein Dieselaggregat abgesichert? ☒ ja ☐ nein
1.9	Werden die Funktionalität 1.2, 1.3, 1.4, 1.6, 1.7 und 1.8, sofern vorhanden, regelmäßig getestet? ☒ ja ☐ nein
2	**Backup- und Notfall-Konzept, Virenschutz**
2.1	Existiert ein Backupkonzept? ☒ ja ☐ nein

2.2	Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet? ☒ ja ☐ nein
2.3	In welchem Rhythmus werden Backups vom Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden? ☐ Echtzeitspiegelung ☒ täglich ☐ ein bis dreimal pro Woche ☐ Sonstiges: bitte angeben
2.4	Auf was für Sicherungsmedien werden die Backups gespeichert? ☒ Zweiter redundanter Server ☐ Sicherungsbänder ☒ Festplatten ☐ Sonstiges: bitte angeben
2.5	Wo werden die Backups aufbewahrt? ☒ Zweiter redundanter Server steht an einem anderen Ort ☐ Safe, feuerfest, datenträger- und dokumentensicher ☐ einfacher Safe ☐ Bankschließfach ☐ abgeschlossener Aktenschrank / Schreibtisch ☐ Im Serverraum ☐ Privathaushalt ☐ Sonstiges: bitte Art der Aufbewahrung angeben
2.6	**Zu 2.5:** 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
2.7	Sind die Backups verschlüsselt? ☒ ja ☐ nein
2.8	Befindet sich der Aufbewahrungsort der Backups in einem vom primären Server aus betrachtet getrennten Brandabschnitt bzw. Gebäudeteil? ☒ ja ☐ nein
2.9	Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement? ☒ ja ☐ nein ☐ Prozess existiert, ist jedoch nicht dokumentiert
2.10	**Wenn 2.9 ja**, wer ist für das Software- bzw. Patchmanagement verantwortlich? ☐ Anwender selbst ☒ eigene IT ☐ Externer Dienstleister
2.11	Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)? ☒ ja ☐ nein
2.12	Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisiertem ☒ Virenschutz ☐ Anti-Spyware ☒ Spamfilter
2.13	**Wenn 2.13 ja**, wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter verantwortlich? ☐ Anwender selbst ☒ eigene IT ☐ Externer Dienstleister
3	**Netzanbindung**
3.1	Verfügt das Unternehmen über eine redundante Internetanbindung? ☐ ja ☒ nein
3.2	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden? ☐ ja ☒ nein
3.3	Wer ist für die Netzanbindung des Unternehmens verantwortlich?

	☐ eigene IT ☒ Externer Dienstleister

2 Beschreibung der einzelnen Maßnahmen

Organisation der Informationssicherheit

IT-Sicherheit und Datenschutz sind bei der Content Optimizer GmbH direkt im Veranwortungsbereich der Geschäftsführung zugeordnet.

Datenschutz und IT-Sicherheit sind definierte Ziele unseres Wertbildes und die Geschäftsführung berücksichtigt die Auswirkungen von Entscheidungen hinsichtlich dieser Werte bei allen Entscheidungen. Im Zweifel wird der Erreichung der Ziele Vorrang eingeräumt.

Die Geschäftsführung und die Mitarbeiter informieren sich laufend über neue Entwicklungen im Datenschutzbereich und prüfen den sich daraus eventuell ergebenden Handlungsbedarf.

Für die korrekte Behandlung von Vorfällen (IT-Sicherheits-, Datenschutz-Verstöße) liegen Verfahrensanweisungen vor. Diese legen fest, wer, wann und unter welchen Umständen zu informieren ist (Kunde, Betroffene, Behörden sowie eigene Mitarbeiter).

Für alle umgesetzten IT-Projekte liegt ein Schwerpunkt bereits in der Planungsphase in einer datenschutzfreundlichen Umsetzung.

Personalsicherheit

Wir wählen Mitarbeiter mit großer Sorgfalt aus. Dabei spielen neben der fachlichen Eignung auch die kommunizierte Bereitschaft zur ständigen Fortbildung eine Rolle.

Vor Aufnahme der Tätigkeit unterschreiben alle Mitarbeiter eine Vertraulichkeits- und Datenschutzvereinbarung, die auch über das Ende des Beschäftigungsverhältnisses hinaus gilt.

Die Mitarbeiter werden im Bereich Datenschutz geschult und regelmäßig sensibilisiert.

Verwaltung der Werte

Sämtliche Werte (wie z. B. Betriebsmittel, Wechseldatenträger, Notebooks) und Datenträger, die mit personenbezogenen Daten in Zusammenhang stehen, werden von uns inventarisiert und sorgfältig behandelt.

Wir haben zum Schutz dieser Werte Verantwortliche festgelegt, die für den Lebenszyklus eines Wertes zuständig sind.

Es wurden dokumentierte Regeln für den zulässigen Gebrauch unserer Werte aufgestellt. Die Rückgabe erfolgt dokumentiert.

Unsere Informationen und Daten werden anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert und gekennzeichnet.

Diesem Klassifizierungsschema entsprechend, haben wir dokumentierte Verfahren für die Handhabung unserer Werte, insbesondere auch unserer Wechseldatenträger, entwickelt und umgesetzt. Wir verfügen über einen dokumentierten und geregelten Prozess zum Transport von Datenträgern, um diese vor unbefugtem Zugriff, Missbrauch oder Verfälschung zu schützen.

Nicht mehr benötigte Datenträger entsorgen wir sicher, unter Anwendung eines dokumentierten Verfahrens und verpflichteter zertifizierter Dienstleister.

Zugangssteuerung

Wir verfügen über geregelte und dokumentierte Maßnahmen, die sicherstellen, dass berechtigte Personen nur auf solche personenbezogenen Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.

Berechtigungen zum Zugriff auf IT-Systeme werden über ein geregeltes Verfahren auf der Grundlage eines dokumentierten und restriktiven Berechtigungskonzepts vergeben. Den Zugang zu Netzwerken und Netzwerkdiensten haben wir geregelt und umgesetzt.

Es ist sichergestellt, dass nur befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird, insbesondere besteht ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern, der die Zuordnung von Zugangsrechten ermöglicht.

Unsere administrativen Rechte erteilen wir eingeschränkt und gesteuert. Wir verfügen über einen dokumentierten und geregelten Prozess über den Umgang mit Passwörtern.

Wir schränken den Zugriff auf unsere Daten bedarfsgerecht ein und steuern den Zugang auf unsere Systeme und Anwendungen durch ein sicheres Anmeldeverfahren. Wir verwenden ein System zur Nutzung sicherer und starker Kennwörter.

Wo immer technisch möglich, ersetzen wir Passwörter durch zertifikatsbasierte Logins.

Kryptographie

Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt.

Verbindungen zu Servern und anderen Einrichtungen des Rechenzentrums erfolgen grundsätzlich über verschlüsselte Verbindungen.

Alle öffentlich zugänglichen Applikationen und Websites verwenden SSL Verschlüsselung für den Datentransport.

Backups, die auf Remote-Servern gespeichert werden, werden grundsätzlich vor der Speicherung verschlüsselt.

Physische und umgebungsbezogene Sicherheit

Wir haben dokumentierte Maßnahmen getroffen, die einen unbefugten Zutritt zu Datenverarbeitungsanlagen oder solchen Einrichtungen in unseren Büroräumen verhindern sollen.

- Die Büroräume verfügen über eine definierte Anzahl Schlüsseln, deren Besitz jederzeit nachvollziehbar ist.
- Die Eingangstür ist in einbruchshemmender Ausführung gefertigt.
- Server, Speicher, Router sowie weiteres kritisches IT-Equipment ist in stets verschlossenen Serverschränken untergebracht um ein beiläufiges entwenden, beschädigen oder manipulieren durch unberechtigte Personen zu verhindern.
- Alle beweglichen Speichermedien sowie Sicherheits-Tokens werden ausserhalb der Nutzung in einem feuergeschützten Safe aufbewahrt. Dies gilt besonders für Zeiträume ausserhalb der Geschäftszeiten.
- Bewegliche Speichermedien sowie Notebook-Festplatten werden grundsätzlich mit aktivierter Verschlüsselung genutzt. Für USB-Sticks und externe Festplatten verwenden wir entweder Veracrypt oder die eingebaute Hardware-Verschlüsselung (mindestens AES-128) oder für die Weitergabe an Kunden einzeln verschlüsselte ZIP-Archive (AES-256). Bei Notebooks verwenden wir die Verschlüsselung des OS (Bei Windows z.B. Bitlocker).
- Die Sicherheit der Server für den Kundeneinsatz stützt sich auf die Sicherheitsmaßnahmen der gewählten Rechenzentrumsbetreiber (Webhoster). Diese sind nach ISO 27001 zertifiziert.
- Für die Vernichtung von Dokumenten und Datenträgern gem. DIN 66399 gilt:
    - In unseren Büros: Sicherheitsstufe 4; Schutzklasse 2&3 (P-4, O-4, T-4, H-4, E-4)
      Papier: Partikelgröße max. 160mm² (typisch 32 mm²)
      Datenträger: physikalische Zerstörung vor Ort in Partkel < 30mm²
    - Im Rechenzentrum unseres Webhosters: gemäß der TOMs des Providers
- Die Webhoster sorgen vertragsgemäß für eine redundante Anbindung der Server an das Internet.
- Die Anbindung der Verwaltung in den Büroräumen erfolgt über eine redundante Verbindung des Telekommunikationsdienstleisters.

Betriebssicherheit

Wir verfügen über geregelte und dokumentierte Maßnahmen, um einen ordnungsgemäßen und sicheren Betrieb von informations- und datenverarbeitenden Einrichtungen sicherzustellen. Diese umfassen u. a. die Steuerung im Falle einer Änderung an den informationsverarbeitenden Einrichtungen, als auch eine Steuerung und regelmäßige Messung unserer Kapazitäten und Ressourcen, um die Verfügbarkeit der erforderlichen Systemleistung sicherzustellen. So werden z. B. unter anderem folgende Werte laufend aktuell überwacht:

- Festplattenstatus und verfügbarer Speicher
- Raid-Status

- Dienste und Status aller virtuellen Maschinen und dedizierten Server
- Speicherbelegung der Storages und Hauptspeicher
- Auslastung Ethernet
- Erreichbarkeit aller Server über SSH
- Verfügbarkeit des Mailservices (intern wie extern)

Ein geschütztes Verfahren zur Datensicherung wurde von uns implementiert und ist dokumentiert.

Standardwartungsfenster sind definiert. Zusätzlich notwendige Fenster werden mindestens 3 Tage vorab angekündigt.

In unserem Unternehmen ist es essentiell, Entwicklungs-, Test und Betriebsumgebungen voneinander getrennt zu halten, so dass wir ein besonderes Augenmerk auf die Einhaltung dieser Trennung haben.

Maßnahmen zur Erkennung, Vorbeugung und Wiederherstellung zum Schutz von Schadsoftware wurden getroffen und werden regelmäßig aktualisiert.

Die Synchronisation unserer Uhren erfolgt zentral mit eines über das Internet angebundenen Zeitservers.

Wir verfügen über ein zentrales Verfahren zur gesteuerten Installation von Software auf Systemen in unserem Unternehmen.

Regelungen für die Einschränkungen von Softwareinstallationen sind von uns zentral dokumentiert.

Kommunikationssicherheit

Die Sicherheit unserer in Netzwerken und Netzwerkdiensten gespeicherten personenbezogenen Daten und Informationen ist unumgänglich. Daher haben wir dokumentierte Maßnahmen eingesetzt, die unsere Netzwerke verwalten, steuern und sichern.

Informationsdienste, Benutzer und Informationssysteme werden bedarfsgerecht, soweit wie möglich, voneinander getrennt gehalten.

Wir verfügen über Richtlinien und Verfahren für die Informations- und Datenübertragung, sowie die Vereinbarungen zur Informationsübertragung an externe Stellen.

Unsere elektronische Nachrichtenübermittlung wird angemessen geschützt. So haben wir unter anderem Maßnahmen zum Schutz der Nachrichten vor unbefugtem Zugriff, vor Veränderung oder Denial of Service getroffen, die dem von der Organisation übernommenen Klassifizierungsschema entsprechen.

Um unsere Daten zu schützen, schließen wir bedarfsgerechte Vertraulichkeits- oder Geheimhaltungsvereinbarungen ab.

Anschaffung, Entwicklung und Instandhaltung von Systemen

Es ist sichergestellt, dass Daten- und Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus unserer Systeme ist. Dies beinhaltet auch die Anforderungen an und die Sicherung von Informationssystemen, die Dienste über öffentliche Netze bereitstellen.

Bei Änderungen an Betriebsplattformen werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationssicherheit gibt.

Wir verfügen über einen definierten Prozess zur Analyse, der Entwicklung und der Pflege sicherer IT Systeme.

Lieferantenbeziehungen

Wir wählen unsere Lieferanten im Vorfeld sorgsam aus und überprüfen ihre Geeignetheit hinsichtlich der Wahrung des Daten- und Informationssicherheitsschutzes.

Dokumentierte Vereinbarungen (Verträge zur Auftragsverarbeitung) sichern den Schutz und die Geheimhaltung unserer Werte und Daten. Die Lieferanten werden verpflichtet, technisch-organisatorische Maßnahmen zu treffen, um dies zu gewährleisten.

Es besteht eine reglementierte und benutzerdefinierte Zugriffsberechtigung auf die für den jeweiligen Lieferanten zwingend benötigten Werte und Daten.

Lieferanten dürfen weitere Lieferanten lediglich mit unserer Zustimmung beauftragen, um eine sichere Lieferkette zu gewährleisten.

Regelmäßig führen wir eine Überprüfung der Datenschutz- und Datensicherheitsmaßnahmen unserer Lieferanten durch, um das vereinbarte Niveau aufrecht zu erhalten. Auch die zugewiesenen Berechtigungen unterliegen einer ständigen dokumentierten Kontrolle.

Nach Beendigung des Lieferantenverhältnisses sind diese Lieferanten verpflichtet, die von uns erhaltenen Daten und Werte an uns zurückzugeben oder ordnungsgemäß zu vernichten. Zudem gilt die Wahrung der Geheimhaltungspflicht in der Regel unbegrenzt.

Handhabung von Informationssicherheitsvorfällen

Unser Unternehmen verfügt über einen geregelten dokumentierten Prozess für die Handhabung von Informationssicherheits- und Datenschutzvorfällen, um diesbezüglich eine konsistente und wirksame Herangehensweise zu gewährleisten.

Die Mitarbeiter sind angehalten, sämtliche Datenschutz- und Sicherheitsereignisse unverzüglich zu melden und werden diesbezüglich regelmäßig geschult.

Sämtliche Ereignisse werden dokumentiert, klassifiziert und bewertet.

Das implementierte Interventionsteam hat genaue Vorgaben, wie auf ein Ereignis zu reagieren ist.

Zusammen mit der Geschäftsleitung werden regelmäßig Verbesserungsmaßnahmen besprochen und umgesetzt, die sich aus den Erkenntnissen und den gesammelten Beweisen eines Ereignisses ergeben.

Informationssicherheitsaspekte beim Business Continuity Management

Im Rahmen der Informationssicherheit wird die vorgesehene Verfügbarkeit von Systemen eigens bewertet und dokumentiert.

Aus den Anforderungen leiten wir die technischen und organisatorischen Vorgaben, wie redundante Systeme/Anbindungen oder entsprechende Planungen ab und setzen diese konsequent und gesteuert um.

Ein übergreifender Notfallplan bildet den Rahmen bezüglich der entsprechenden Handlungsanweisungen für ausgewählte dokumentierte Notfallszenarien.

Laufende aktualisierte Übungspläne für die Erprobung der eingesetzten Maßnahmen und die Dokumentation der Durchführung entsprechender Tests rundet das Notfallmanagement ab.

Compliance

Wir haben alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen unseres Unternehmens zur Einhaltung dieser Anforderungen bestimmt, dokumentiert und halten diese auf dem neuesten Stand.

Entsprechend der gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen schützen wir Aufzeichnungen und personenbezogene Daten bedarfsgerecht.

Anlage 2 – Zugelassene Subdienstleister

Unternehmen	Funktion / Zweck	Kontaktdaten Beschreibung Anmerkungen
Schlund Technologies GmbH	Domain-Providing	https://www.schlundtech.de/ Standort: Deutschland
Host Europe GmbH	Webhoster	https://www.hosteurope.de/ Standort: Deutschland
OVH GmbH	Webhoster	https://www.ovh.de/ Standort: Deutschland
Hetzner Online GmbH	Webhoster	https://www.hetzner.com/ Standorte: Deutschland und andere EU.

Anlage 3 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Beim Kunden

Vorname Name	E-Mail-Adresse	Telefonnummer

Beim Auftragnehmer

Vorname Name	E-Mail-Adresse	Telefonnummer
Dominik Belca	dbelca@content-optimizer.de	0201-87659865
Kerstin Belca	kbelca@content-optimizer.de	0201-87659865
Sebastian Fahrenkrog	sfahrenkrog@content-optimizer.de	0201-87659865