Vereinbarung über Auftragsverarbeitung

ZWISCHEN

NAME ODER FIRMA

STRASSE UND NR.

PLZ UND ORT

LAND

- nachstehend Auftraggeber genannt -

UND

Firma Code Piraten GmbH, vertreten durch Herrn Stefan Wirtz, Am Ruhmbach 44, 45149 Essen,
- nachstehend Auftragnehmer genannt -

MUSTER

§ 1 Gegenstand des Auftrages

(1) Gegenstand des Auftrages ist dem jeweiligen Leistungsvertrag der Parteien zu entnehmen.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers. Bei dem Vertragsgegenstand handelt es sich deshalb um eine Auftragsverarbeitung. Die Parteien sind sich darin einig, dass auf diesen Vertrag ab dem 25.05.2018 die Vorschriften der EU-Datenschutzgrundverordnung (DSGVO), insbesondere die Vorschriften über die Datenverarbeitung im Auftrag, anzuwenden sind. Der Auftragnehmer erklärt, dass er in der Lage ist, die aufgetragenen Leistungen nach Maßgabe des Art. 28 DSGVO ordnungsgemäß durchzuführen.

(3) Der Vertrag regelt die datenschutzrechtlichen Maßnahmen im Sinne von Art. 28 DSGVO und §80 SGB X und die Rechte und Pflichten des Auftraggebers und des Auftragnehmers zur Erfüllung der datenschutzrechtlichen Anforderungen.

§ 2 Dauer, Laufzeit des Auftrages, Zweck

Die Laufzeit dieses Vertrages ist an die Laufzeit des Leistungsvertrages geknüpft.
Zweck der Verarbeitung ist ausschließlich die Durchführung der im Leistungsvertrag vereinbarten Leistungen. Eine Verarbeitung zu eigenen oder anderen Zwecken des Auftragnehmers ist unzulässig.

§ 3 Kategorien von betroffenen Personen

Die Auftragserfüllung und Datenverarbeitung durch den Auftragnehmer kann folgende Kategorien von natürlichen Personen des Auftraggebers betreffen:

(Bitte die Kategorien von natürlichen Personen angeben, welche durch die Auftragsausführung des Auftragnehmers betroffen sein können)

§ 4 Arten der personenbezogenen Daten

(1) Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien:

(Bitte die personenbezogenen Daten oder zumindest die Datenkategorien, welche der Auftragnehmer bei der Auftragsausführung gegebenenfalls zur Kenntnis nehmen kann, hier eintragen).

§ 5 Ort der Verarbeitung

(1) Die Datenverarbeitung findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland oder innerhalb der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes statt. Eine Verarbeitung in anderen Staaten ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist. Der Auftragnehmer führt auf Wunsch des Auftraggebers den Nachweis für das Bestehen eines Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO und/oder der Garantien und eines angemessenen Schutzniveaus.

Der Nachweis kann **durch Vorlage eines entsprechenden Zertifikates einer akkreditierten Zertifizierungsstelle nach Art. 43 DSGVO geführt werden. Der Auftragnehmer verpflichtet sich, die Einhaltung der Garantien und eines angemessenen Schutzniveaus sicherzustellen. Der Auftraggeber behält sich vor, das Vorliegen des Angemessenheitsbeschlusses der EU-Kommission sowie, der Garantien und die Einhaltung eines angemessenen Schutzniveaus im Rahmen seiner Audit- und Kontrollrechte jederzeit zu überprüfen.**

§ 6 Kontroll- und Auditrechte des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung der personenbezogenen Daten sowie für die Ausführung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Bei einer Datenverarbeitung im Auftrag arbeitet der Auftraggeber gem. Art. 28 Abs. 1 Satz 1 DSGVO nur mit Auftragsverarbeitern zusammen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen zur Erfüllung der Anforderungen der DSGVO eingerichtet sind.

(2) Der Auftraggeber ist danach befugt, vor Beginn der Datenverarbeitung und nach seinem Ermessen auch wiederholt nach vorheriger Abstimmung während der üblichen Geschäftszeiten im erforderlichen Umfang die Einhaltung der Vorschriften

über den Datenschutz und der vertraglichen Vereinbarungen, insbesondere der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen, zu kontrollieren.

Hierzu ist der Auftraggeber befugt, schriftliche Auskünfte und die Vorlage von Nachweisen über die eingerichteten Datenschutzmaßnahmen sowie über die Art und Weise ihrer technischen und organisatorischen Umsetzung zu verlangen, das Grundstück und die Betriebsstätten des Auftragnehmers zu betreten, nach seinem Ermessen Prüfungen und Besichtigungen vorzunehmen und im erforderlichen Umfang in verarbeitungsrelevante Unterlagen, Verarbeitungs- und Ablaufprotokolle, Systeme und gespeicherte Daten und in Regelungen, Richtlinien und Handbücher zur Regelung der beauftragten Datenverarbeitung einzusehen. Dazu gehören auch Nachweise über die Bestellung eines Datenschutzbeauftragten (sofern notwendig), die Verpflichtung der Mitarbeiter auf die Wahrung der Vertraulichkeit und technische und organisatorische Konzepte, z.B. Verträge mit Unterauftragnehmern. Die gleichen Rechte besitzen auch Beauftragte des Auftraggebers, z. B. Gutachter oder Sachverständige, soweit sie besonders zur Verschwiegenheit verpflichtet sind oder strafbewehrten berufsständischen Schweigepflichten unterliegen.

(3) Die Rechte des Auftraggebers bestehen während der Laufzeit dieser Vereinbarung und darüber hinaus bis zum Eintritt der Verjährung von Ansprüchen aus diesem Vertrag, mindestens jedoch solange der Auftragnehmer personenbezogene Daten aus den beauftragten Verarbeitungen speichert.

(4) Die Prüfung erfolgt nach vorheriger Anmeldung. In besonderen Fällen, insbesondere wenn Verarbeitungsprobleme bestehen, meldepflichtige Vorfälle aufgetreten sind oder aufsichtsrechtliche Maßnahmen anstehen oder eingeleitet worden sind, kann die Prüfung auch ohne vorherige Anmeldung erfolgen.

MUSTER

§ 7 Weisungsbefugnisse des Auftraggebers

(1) Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Leistungsvereinbarungen und dieser Vereinbarung über Auftragsverarbeitung nur auf dokumentierte Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der getroffenen Auftragsbeschreibung ein Weisungsrecht in Form von Einzelanweisungen über einzelne datenverarbeitende Prozesse des Auftragnehmers vor. Die Weisungen werden schriftlich, in Schriftform oder in einem anderen geeignetem elektronischem Format erteilt. Mündliche Weisungen werden unverzüglich in Schriftform, schriftlich oder in einem elektronischen Format bestätigt. Die Weisungen werden über die Dauer des Auftragsverhältnisses, mindestens jedoch für die Dauer ihrer Gültigkeit, aufbewahrt.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzvorschriften verstößt. Der Auftragnehmer kann die Ausführung der Anweisung bis zu einer Bestätigung durch den Auftraggeber aussetzen.

Weisungsberechtigte Personen des Auftraggebers sind:

BITTE HIER DIE NAMEN EINTRAGEN.

Weisungsempfänger beim Auftragnehmer sind: Stefan Wirtz, Patrick Seiferth

Änderungen der weisungsberechtigten Personen oder der Weisungsempfänger sind unverzüglich mitzuteilen.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

§ 8 Pflichten des Auftragnehmers

(1) Verarbeitungspflichten

Der Auftragnehmer führt den Auftrag ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Auszüge, Kopien oder Duplikate von Daten oder Datenträgern dürfen ohne Wissen des Auftraggebers nur hergestellt und verwendet werden, soweit dies für die Ausführung des Auftrages oder zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich ist oder eine gesetzliche Aufbewahrungspflicht besteht. Eventuell hergestellte Auszüge, Kopien oder Duplikate sind nach Abschluss der Verarbeitung oder Nutzung vom Auftragnehmer unverzüglich sicher zu löschen bzw. datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nicht oder nur nach Weisung des Auftraggebers erteilen. Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen erteilen.

Der Auftragnehmer verpflichtet sich, nur solche Software, Daten oder Datenträger einzusetzen, die zuverlässig auf Freiheit von schädlicher Software geprüft sind, um ein Einschleusen von Viren etc. zu vermeiden.

(2) Duldungspflichten bei Kontrollen

Der Auftragnehmer verpflichtet sich, in Prüfungen durch den Auftraggeber die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nachzuweisen, Auskünfte zu erteilen und die entsprechenden Unterlagen vorzulegen bzw. Einsicht in die erforderlichen Unterlagen und Systeme zu gewähren und nach vorheriger Abstimmung entsprechende Prüfungen des Auftraggebers vor Ort zu dulden und zu unterstützen. Er verpflichtet sich, bei datenschutz- und datensicherheitsrelevanten Vorfällen alle erforderlichen Auskünfte zu erteilen und die Aufklärung derartiger Vorfälle nach Möglichkeit zu unterstützen.

Der Nachweis angemessener technischer und organisatorischer Maßnahmen kann auch durch Vorlage von Testaten oder Zertifikaten oder durch eine Zertifizierung bzw. ein Datenschutzaudit einer unabhängigen Einrichtung bzw. eines autorisierten Sachverständigen geführt werden. Unabhängig von diesen Nachweisen ist der Auftragnehmer verpflichtet, Kontrollen durch den Auftraggeber gem. § 6 dieser Vereinbarung zu dulden.

MUSTER

(3) Informationspflichten

Der Auftragnehmer ist verpflichtet, wesentliche Änderungen in den technischen und organisatorischen Verhältnissen, die die Sicherheit und Ordnungsmäßigkeit der Durchführung der Auftragsleistungen herabsetzen, unaufgefordert dem Auftraggeber zu melden.

Der Auftragnehmer unterrichtet den Auftraggeber über Kontrollen der Aufsichtsbehörde für den Datenschutz, insbesondere gem. Art. 58 DSGVO, und über eventuelle Maßnahmen und Auflagen zum Schutz der personenbezogenen Daten.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Er informiert den Auftraggeber unverzüglich über das Erlöschen oder den Widerruf von Zertifikaten oder von Maßnahmen gem. Art. 41 Abs. 4 DSGVO.

Der Auftragnehmer teilt dem Auftraggeber Name und Kontaktdaten und Änderungen in der Person des betrieblichen Datenschutzbeauftragten oder, wenn keine Bestellpflicht besteht, den Namen und die Kontaktdaten der sonstigen zuständigen Stelle mit.

(4) Mitwirkungs- und Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen im notwendigen Umfang bei der Erfüllung der in Artikel 35 und 36 DSGVO genannten Pflichten (Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsichtsbehörde).

Sofern eine vom Verantwortlichen durchgeführte Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO ergibt, dass die Verarbeitung trotz der vom Verantwortlichen vorgesehenen Maßnahmen zur Risikominderung ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen zur Folge hätte, und der Verantwortliche daher eine vorherige Konsultation der zuständigen Datenschutzaufsichtsbehörde gemäß Art. 36 DSGVO durchführt, wird der Auftragsverarbeiter dem Verantwortlichen auf Anforderung alle für diese Konsultation erforderlichen Informationen und Dokumentationen aus seinem Verantwortungsbereich unverzüglich zur Verfügung stellen. Dies umfasst insbesondere Angaben zu den technischen und organisatorischen Sicherheitsmaßnahmen (TOM) sowie zu den vom Auftragsverarbeiter eingesetzten Verarbeitungsabläufen.

Der Auftragsverarbeiter benennt dem Verantwortlichen auf Anfrage einen qualifizierten Ansprechpartner, der für Rückfragen der Aufsichtsbehörde im Rahmen des Konsultationsverfahrens nach Art. 36 DSGVO über den Verantwortlichen zur Verfügung steht.

Der Auftragsverarbeiter ist berechtigt, für die Erbringung von Unterstützungsleistungen im Rahmen dieses Paragraphen, die über die bloße Bereitstellung von Standarddokumentationen hinausgehen, eine angemessene Vergütung nach tatsächlichem Aufwand zu verlangen, es sei denn, die Notwendigkeit der Konsultation beruht auf einem schuldhaften Fehlverhalten des Auftragsverarbeiters.

(5) Organisationspflichten

Der Auftragnehmer verpflichtet sich zur Einrichtung von Maßnahmen und Dokumentationen, die eine Kontrolle und Nachvollziehbarkeit aller mit der Auftragsverarbeitung zusammenhängenden Tätigkeiten und Verarbeitungsprozesse im Sinne einer Auftragskontrolle und der Ordnungsmäßigkeit der Datenverarbeitung ermöglichen. Datenschutzvorfälle und sonstige sicherheitsrelevante Störungen der Verarbeitung sind einschließlich ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen zu dokumentieren und dem Auftraggeber zu melden. Die Dokumentation ist dem Auftraggeber unverzüglich zur Verfügung zu stellen.

Wird die Verarbeitung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, verpflichtet sich der Auftragnehmer, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Verarbeitung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung vom Ort des Auftragnehmers aus der Fall ist.

§ 9 Wahrung der Vertraulichkeit und sonstiger Geheimnisse

(1) Personenbezogene und sonstige Daten oder Informationen, die dem Auftragnehmer im Rahmen der Erfüllung dieses Vertrags bekannt werden, darf der Auftragnehmer nur für Zwecke der beauftragten Leistung verwenden. Der Auftragnehmer verpflichtet sich, die Vertraulichkeit und Integrität der personenbezogenen Daten zu wahren und alle ihm im Zusammenhang mit der Übernahme und Abwicklung des Auftrages bekannt werdenden personenbezogenen Daten und sonstige unternehmensinterne Umstände, Daten und Informationen (Betriebsgeheimnisse) vertraulich zu behandeln sowie die im Rahmen dieses Vertrages tätig werdenden Mitarbeiter auch über die Beendigung des Beschäftigungsverhältnisses hinaus auf die Wahrung der Vertraulichkeit schriftlich zu verpflichten und über die Datenschutzpflichten aus diesem Vertrag, die Weisungsgebundenheit der Verarbeitung der Daten und deren Zweckbindung zu belehren. Diese Geheimhaltungspflicht gilt auch über die Beendigung des Vertragsverhältnisses hinaus.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er für die Durchführung der Arbeiten nur eigenes Personal einsetzt und die mit der Auftragsdurchführung beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und einer regelmäßigen Schulung unterzieht.

(3) Der Auftragnehmer verpflichtet sich zur Beachtung aller sonstigen Geheimnisse, soweit diese für die Verarbeitung einschlägig sind, wie des Sozialgeheimnisses, des Fernmeldegeheimnisses und sonstiger Berufsgeheimnisse gem. § 203 StGB sowie zur Verpflichtung und Belehrung der Beschäftigten zur Sicherstellung der Wahrung dieser Geheimnisse.

MUSTER

(4) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über administrative Zugangsdaten und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen. Von den ihm eingeräumten Zugriffsrechten darf der Auftragnehmer nur in dem Umfang Gebrauch machen, der für die Durchführung der Datenverarbeitung erforderlich ist. Die Verpflichtung zur Wahrung der Vertraulichkeit und der sonstigen Geheimnisse gilt auch über die Beendigung dieses Vertrages hinaus.

§ 10 Unterauftragsverhältnisse

(1) Mit Unterzeichnung dieses Vertrages stimmt der Auftraggeber der Einschaltung der in der Anlage 2 im Einzelnen aufgeführten Unterauftragnehmer zu.

(2) Im Fall der Einschaltung von weiteren Unterauftragnehmern, wird der Auftragnehmer die Unterauftragnehmer nach deren Eignung sorgfältig auswählen. Für die Einschaltung von Unterauftragnehmern, welche eine Datenverarbeitung ausschließlich innerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR) garantieren und auch sämtliche Voraussetzungen für eine rechtskonforme Datenverarbeitung erfüllen, erteilt der Auftraggeber hiermit bereits jetzt ausdrücklich seine Zustimmung. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung dieser Auftragsverarbeiter rechtzeitig informieren, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Hinzuziehungen bzw. Änderungen innerhalb einer gesetzten Frist Einspruch zu erheben. Die Einschaltung von Unterauftragnehmern außerhalb der EU und des EWR (auch im Falle von verbundenen Unternehmen) bedarf der ausdrücklichen vorherigen schriftlichen Einwilligung des Auftraggebers.

(3) Der Auftraggeber kann bei Vorliegen eines von ihm nachzuweisenden wichtigen Grundes, insbesondere bei einer Gesetzes- oder Vertragsverletzung, seine Zustimmung zur Unterbeauftragung widerrufen. Die Unterbeauftragung ist dann unverzüglich einzustellen.

(4) Der Auftragnehmer hat die vertraglichen Vereinbarungen mit jedem Unterauftragnehmer so zu gestalten, dass sie den Datenschutzbestimmungen dieses Vertrages in vollem Umfang entsprechen. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten an einen Unterauftragnehmer ist erst zulässig, wenn eine entsprechende Vereinbarung über eine Auftragsverarbeitung abgeschlossen worden ist und der Unterauftragnehmer alle Anforderungen dieses Vertrages erfüllt hat. Auf schriftliche Anforderung hat der Auftragnehmer dem Auftraggeber Auskunft über die wesentlichen Vertragsinhalte und die Umsetzung der datenschutzrelevanten Verpflichtungen der Unterauftragsverhältnisse, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erteilen.

(5) 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, Wartung und Benutzerservice, Reinigungskräfte. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremdvergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(6) Eine Beauftragung von Unterauftragnehmern außerhalb des Gebiets der Bundesrepublik Deutschland oder der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraumes ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist. Im Übrigen gelten die Regelungen zu § 5 dieses Vertrages auch für die Beauftragung von Unterauftragnehmern.

§ 11 Mitteilungspflichten bei Störungen und Datenschutzverletzungen

(1) Bei einer Störung der Verarbeitung oder einer Datenschutzverletzung leitet der Auftragnehmer umgehend alle geeigneten und erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung eines eventuellen Schadens für die Betroffenen und für den Auftraggeber ein.

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich über Verstöße gegen Vorschriften zum Schutz der personenbezogenen Daten oder gegen die in dieser Vereinbarung getroffenen Festlegungen wie folgt zu unterrichten:

(bitte Kommunikationskanal, z.B. E-Mailadresse für Meldungen, ergänzen)

Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder andere Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers, die Auswirkungen auf die betroffenen Personen oder den Auftraggeber nach sich ziehen oder Schaden verursachen können. Zu den Datenschutzverstößen gehören insbesondere der Verlust der Vertraulichkeit und der Verlust oder die Zerstörung oder Verfälschung von Daten des Auftraggebers oder sonstiger vertraulicher Informationen im Sinne dieses Vertrages.

(3) Die Meldung an den Auftraggeber umfasst alle Informationen, die für den Auftraggeber erforderlich sind, um den Vorfall und seine Meldepflicht an die Aufsichtsbehörde und die Informationspflicht der Betroffenen gem. Art. 33 und 34 DSGVO beurteilen und ggf. fristgerecht die Meldung an die Aufsichtsbehörde und ggf. die Information der Betroffenen vornehmen zu können. Die Meldung an den Auftraggeber umfasst insbesondere Angaben zur Art des Vorfalls und der Verletzung des Schutzes von personenbezogenen

MUSTER

Daten, eine Beschreibung der wahrscheinlichen Risiken für die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen und eine Beschreibung der bereits eingeleiteten Maßnahmen zur Behebung bzw. Reduzierung eines möglichen Schadens oder sonstiger Risiken für die Betroffenen und den Auftraggeber.

(4) Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Informationspflicht gem. Art. 33 und 34 DSGVO und unternimmt alle in seinen Verantwortungsbereich fallenden Maßnahmen zur Minderung nachteiliger Folgen für die Betroffenen sowie zur Aufklärung des Vorfalls und dessen Folgen. Dies gilt auch nach Beendigung des Vertragsverhältnisses.

§ 12 Rechte der Betroffenen

(1) Für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und zuständig. Der Auftragnehmer darf Rechte der Betroffenen nur nach Weisung des Auftraggebers umsetzen. Der Auftragnehmer unterstützt jedoch den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen im notwendigen Umfang.

(2) Anfragen von Betroffenen zu ihren Rechten oder von einem Betroffenen verlangte Auskünfte, Berichtigungen, Löschungen von Daten werden vom Auftragnehmer unverzüglich an den Auftraggeber zur Erledigung weitergeleitet. Auskünfte an Dritte dürfen nur nach Weisung des Auftraggebers erteilt werden oder sind an den Auftraggeber zur Erledigung weiterzuleiten. Ebenso dürfen Auskünfte an Beschäftigte des Auftraggebers nicht unmittelbar an diese, sondern nur über die vereinbarten Kontaktpersonen erteilt werden.

§ 13 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer sichert ein dem Risiko für die Rechte und Freiheiten der Betroffenen adäquates Schutzniveau der personenbezogenen Daten zu. Zu diesem Zweck verpflichtet sich der Auftragnehmer, seine innerbetriebliche Organisation und die erforderlichen technischen und organisatorischen Maßnahmen unter Berücksichtigung des jeweiligen Stands der Technik, der Implementierungskosten und der Art, des Umfangs sowie der Umstände und Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen so zu gestalten und laufend zu aktualisieren, dass diese den besonderen Anforderungen des Datenschutzes nach der DSGVO entsprechen und den Schutz der Rechte der betroffenen Personen gewährleisten.

Die technischen und organisatorischen Maßnahmen umfassen insbesondere

a) die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten,

b) die rasche Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen im Fall eines physischen oder technischen Zwischenfalls und

c) die Einführung und das Vorhalten von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Der Auftragnehmer sichert die Einhaltung der in der Anlage 1 genannten technischen und organisatorischen Maßnahmen zu. Diese Maßnahmen gelten als vereinbart und die Beschreibung der Maßnahmen in der Anlage 1 wird Bestandteil dieses Vertrages.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragnehmer kann die Eignung der nach Art. 32 DSGVO zu treffenden technisch-organisatorischen Maßnahmen gegebenenfalls durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO oder eines Datenschutzsiegels oder Prüfzeichen nach Art. 42 DSGVO nachweisen, das für die vertragsgegenständlichen Verarbeitungsverfahren und Orte erteilt und für die unter diese Vereinbarung fallenden Verarbeitungsverfahren relevant ist. Der Auftragnehmer hat Veränderungen am Zertifikat oder dessen Ablauf dem Auftraggeber unverzüglich mitzuteilen. Die Kontroll- und Auditrechte des Auftraggebers bleiben unberührt.

§ 14 Verfahren nach Beendigung des Auftrages

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten personenbezogenen Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Aufforderung durch den Auftraggeber datenschutzgerecht zu vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Natur und dem Zeitpunkt der Löschung.

MUSTER

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

Sollte keine Übergabe der Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, die durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren sind, dann läuft der Vertrag abweichend von § 2 bis zum Ablauf der Aufbewahrungsfristen.

§ 15 Vertragsdauer, Kündigung

(1) Die Vertragsdauer richtet sich nach der Laufzeit des Leistungsvertrages.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers oder eines Unterauftragnehmers gegen datenschutzrechtliche Vorschriften oder gegen diese Vereinbarung vorliegt, der Auftragnehmer oder ein Unterauftragnehmer einer rechtmäßigen Weisung des Auftraggebers nicht nachkommt oder ein Auftragnehmer oder der Unterauftragnehmer sich einer angemessenen Datenschutzkontrolle entzieht.

(3) Eine Kündigung des Vertrags kann nur schriftlich erfolgen.

§ 16 Wirksamkeit der Vereinbarung

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

§ 17 Haftung

Für die Haftung gelten die Regelungen des Art. 82 DSGVO.

§ 18 Namen und Kontaktdaten der zuständigen Stelle beim Auftragnehmer

Herr Stefan Wirtz,Am Ruhmbach 44, 45149 Essen, E-Mail: datenschutz@codepiraten.com

§ 19 Anwendbares Recht und Gerichtsstand

(1) Das anwendbare Recht und der Gerichtsstand richten sich nach den Regelungen des jeweiligen Leistungsvertrages.

(2) Gesetzliche Regelungen über ausschließliche Zuständigkeiten bleiben unberührt.

MUSTER

ESSEN /

ORT/DATUM

CodePiraten
Individuelle Anwendungsentwicklung

UNTERSCHRIFT/STEMPEL AUFTRAGNEHMER

Anlage 1
Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO
Beschreibung der vereinbarten technischen und organisatorischen Maßnahmen

Folgende technische und organisatorische Maßnahmen sind eingerichtet und gelten als vereinbart:

Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht eine Zertifizierung nach DIN EN ISO/IEC 27001:2022
- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogen und mindestens halbjährlich evaluiert wird.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Vertraulichkeit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden existieren spezielle Regelungen („Home-/Mobile- Office-Vereinbarungen“) zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung. Eine Nutzung privater Endgeräte ist verboten.
- Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
- Regelmäßige Schwachstellenanalyse und gegebenenfalls Anpassung von technischen und organisatorischen Maßnahmen zur Datensicherheit durch uns sowie unsere Hoster, die Firmen Hetzner Online GmbH und netcup GmbH (dort sind sämtliche personenbezogenen Daten gespeichert). Beide Hoster sind ISO27001 zertifiziert. Jeweils aktuelle Versionen des „ISO-27001-Zertifikates“ beider Firmen liegen vor.
- Datenschutzfreundliche Voreinstellungen von Softwareentwicklungen
- Laufendes Datenschutzmanagement zur ständigen Aktualisierung des Verarbeitungsverzeichnisses samt vertraglicher Regelungen und organisatorischer Maßnahmen sowie regelmäßige Bewertung und gegebenenfalls Anpassung dieser Maßnahmen durch ext. Datenschutzbeauftragten.
- Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.

Zutrittskontrolle

- Sämtliche Mitarbeiter sind auf Vertraulichkeit verpflichtet.
- Sicherheitsschlösser
- Videoüberwachung
- Alarmanlage

MUSTER

Zugangskontrolle / Zugriffskontrolle

- Tresor für sensible Daten
- Stets aktuelle Softwareversionen
- Firewall (Software)
- Mindestpasswortlängen und Passwortmanager
- Authentifikation mit Benutzer und Passwort und bei erhöhtem Schutzbedarf durch eine zusätzliche Multifaktor-Authentisierung
- Protokollierung von Zugriffen auf Daten
- Automatische Sperrung bei mehrfacher Falscheingabe von Kennwörtern
- Kennwortverfahren für alle Ebenen (lokales Netzwerk, Server, Anwendungen) u.a. mit Sonderzeichen, Mindestlänge und regelmäßigem Kennwortwechsel
- Verschlüsselung von Festplatten (FileVault, Bitlocker)
- Einrichtung eines Benutzerstammsatzes pro User
- Differenzierte Berechtigungsprofile der einzelnen Benutzer, so dass eine Zugriffsberechtigung nur für die Daten besteht, die ein Mitarbeiter zur Aufgabenerledigung benötigt.
- Verschlüsselung von mobilen Datenträgern und Geräten
- Einsatz von VPN-Technologie
- Sämtliche lokalen Rechner sind per Passwort geschützt. Zusätzlich ist die Festplatte verschlüsselt.
- Sämtliche Daten werden über ein CRM (Eigenentwicklung) vollverschlüsselt auf einem Server in einem Rechenzentrum der Firma Hetzner (Serverstandort Deutschland) gespeichert. Die Daten im CRM werden nur von einer Person eingegeben, verändert oder gelöscht. Sie können nur mit den Zugangsdaten dieser Person entschlüsselt werden.
- Sämtliche Mitarbeiter sind auf Vertraulichkeit verpflichtet.
- Mitarbeiter dürfen außerhalb der Büroräume an Projekten arbeiten. Es ist vorgeschrieben, dass keine öffentlichen WLANs genutzt werden dürfen.

Weitergabekontrolle

- Verschlüsselung von Datenträgern und Verbindungen
- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- Elektronische Signatur durch SSL-Zertifikat
- Differenzierte Berechtigungsprofile der einzelnen Benutzer, so dass eine Zugriffsberechtigung nur für die Daten besteht, die ein Mitarbeiter zur Aufgabenerledigung benötigt.

Eingabekontrolle

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Auftragskontrolle

- Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten
- Kontrolle der Vertragsausführung
- Eindeutige Vertragsgestaltung (Arbeitsverträge, Home-Mobile-Office Zusatzvereinbarungen, Gestaltungsrichtlinien für Home-Office, Verschwiegenheitsvereinbarungen, Auftragsverarbeitungsverträge mit Subunternehmern etc.)

MUSTER

Verfügbarkeitskontrolle / Integrität

- Notfallkonzept
- Ständig kontrolliertes Backup- und Recoverykonzept
- Unterbrechungsfreie Stromversorgung und Überspannungsschutz
- Sicherstellung einer funktionsfähigen Klimatisierung
- Einsatz von Festplattenspiegelung
- Eine Backup-Routine sichert die Daten auf einem extra Backup-Space unserer Provider (derzeit die Firmen Hetzner und netcup – siehe Anlage 2). Backups der Rechner der Mitarbeiter werden verschlüsselt übertragen und zusätzlich werden lokale verschlüsselte Sicherungen der Rechner erstellt. Service Desk zur Fehlermeldung
- Ausgiebige Tests von produktiver Inbetriebnahme neuer IT-Systeme
- Eine Backup-Routine sichert die Daten auf einem extra Backup-Space unserer Provider (derzeit die Firmen Hetzner und netcup – siehe Anlage 2).

Gewährleistung des Zweckbindungs-/Trennungsgebotes

- Die Verarbeitung von Daten erfolgt auf Serversystemen, die durch ein System von verschiedenen Zugriffskontrollen und Zugriffsrechten getrennt sind.
- Logische Mandantentrennung (Software)
- Trennung von Produktiv- und Testsystem

MUSTER

Anlage 2
Unterauftragnehmer

Unterauftragnehmer, Name, Adresse	Beauftragte Leistungen	Vertragsbeginn
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	Hosting	16.03.2018
netcup GmbH Daimlerstraße 25 76185 Karlsruhe Deutschland	Hosting	26.12.2024
NUR beim Versand von Push-Benachrichtigungen Für den Versand von Push-Benachrichtigungen an die Endgeräte der Gäste nutzen wir die Dienste Firebase Cloud Messaging (Google Ireland Limited) und den Apple Push Notification service (Apple Distribution International Ltd.). Diese Dienste werden nur dann angesprochen, wenn ein Kunde über unsere API eine Push-Mitteilung an seine Gäste auslöst; dabei werden ausschließlich die für die Zustellung technisch erforderlichen Daten (insbesondere Geräte-/Push-Token und der Nachrichteninhalt) an den jeweiligen Dienst übermittelt. Werden keine Push-Mitteilungen versendet, findet auch keine Verarbeitung durch diese Unterauftragnehmer statt.		
Google Ireland Limited Gordon House, Barrow Street Dublin 4 Irland	ush-Benachrichtigungen (Firebase Cloud Messaging)	06.03.2020
Apple Distribution International Ltd. Hollyhill Industrial Estate, Hollyhill Cork Irland	Push-Benachrichtigungen (Apple Push Notification service)	13.01.2020

MUSTER