Version1 vom 30.01.2020

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen

vertreten durch

im Folgenden: **Auftraggeber**

123NIC.de

Am Kiesgrund 34a

16548 Glienicke Nordbahn

vertreten durch

Detlef Köppel

im Folgenden: **Auftragnehmer**

1 Einleitung, Geltungsbereich, Definitionen

Der Auftraggeber beabsichtigt, den Auftragnehmer im Rahmen der Erfüllung abgeschlossener und/oder noch abzuschließender Einzelverträge unter anderem auch mit der Verarbeitung personenbezogener Daten des Auftraggebers zu beauftragen.

Mit dieser Vereinbarung sollen die datenschutzrechtlichen Rahmenbedingungen und diesbezüglichen Verpflichtungen der Vertragsparteien festgehalten werden, die im Zuge der zukünftigen Beauftragung unverändert Geltung beanspruchen. Diese Vereinbarung findet dabei Anwendung auf alle Tätigkeiten des Auftragnehmers.

Diese Vereinbarung wird ergänzt durch konkrete, auftragsbezogene datenschutzrechtliche Regelungen, die jeweils in einem entsprechenden und auf diesen Auftrag Bezug nehmenden Einzelvertrag getroffen werden

.In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutzgrundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. 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 folgende Verarbeitungen:

Datenverarbeitung im Auftrag ist die Speicherung und automatische Löschung von hochgeladenen Daten durch den Auftraggeber berechtigte, benannte und unbenannte Personen. Auftragsverarbeitung im Sinne der vorliegenden Regelung wird auch die Erhebung oder sonstige Nutzung personenbezogener Daten gefasst. Die Datenerfassung aller Personen bezieht sich lediglich auf eine E-Mailadresse die grundsätzlich so gestaltet sein kann, dass eine namentliche Zuordnung nicht möglich ist. Diese Anonymisierung ist nicht zwingend notwendig wenn der Nutzer seine E-Mail Adresse auf anderen Plattformen, Visitenkarten oder ähnliches veröffentlicht hat. Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag (im Folgenden „Hauptvertrag“).

2.2 Dauer

Die Dauer eines Auftrages ist in dem jeweiligen Einzelvertrag niedergelegt.

3 Art, Zweck, Sicherheit und Betroffene der Datenverarbeitung:

3.1 Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art:

Der Nutzer kann über die bereitgestellte Plattform Daten an einen berechtigten Empfänger des Auftraggebers bis zu einer Größe von 20GB (optional 50GB) je Sendung senden. Die Daten werden bereits beim Upload auf Viren geprüft und mittels Libsodium von Dan Bernstein verschlüsselt. Die Daten werden bereits mit dem ersten Byte verschlüsselt und mit einem 256SHA Hash versehen. Das Hashtag dient der eindeutigen

Identifizierung gegenüber Änderungen nach dem Upload. Zusätzlich kann noch eine Passphrase (Geheimwort) vereinbart werden. Geht das Geheimwort verloren können die Daten nicht wiederhergestellt werden. Das Geheimwort wird nicht gespeichert.

Die Verarbeitung dient folgendem Zweck:

Die Daten werden verschlüsselt auf dem Server gespeichert und sind durch einen Hashtag gesichert. Der Empfänger erhält eine E-Mail mit einer eindeutigen ClaimID sowie ein Passcode. Diese Daten und das Hashtag müssen beim Abholen der Daten übereinstimmen. Stimmen die Daten nicht mehr überein, ist die Sicherheit der Daten nicht mehr gegeben und der Vorgang wird abgebrochen. Ist ein Geheimwort vereinbart muss dieses vor dem Download angegeben werden. Das Geheimwort kennt nur der Absender und muss dem Empfänger entsprechend übermittelt werden. Bestenfalls per Telefon.

Werden Daten zur Übersendung angefordert ist das Geheimwort nur dem Anfordernden bekannt. Dieses Geheimwort wird zum Download der angeforderten Daten benötigt.

3.2 Sicherheit der Daten

Es werden folgende Daten verarbeitet:

- Alle Daten die hochgeladen werden sind verschlüsselt und/oder zusätzlich mit einem Passphrase / Geheimwort geschützt
- Die E-Mailadressen und Namen der berechtigten Empfänger. (Interne)
- Die Emailadressen der Absender werden nur während des Prozesse (Cookie) gespeichert , da eine weitere Identifizierung über die ClamID und Passcode stattfindet.
- Eine Eingabe von weiteren personenbezogenen Daten ist zu keiner Zeit notwendig.
- Benutzer, die sich nicht anmelden können (dh Benutzer, die nicht Mitglieder der Host-Organisation sind), können nur Dateien an Personen senden, die Mitglieder der Host-Organisation sind. Es kann nicht verwendet werden, um Dateien von einem Nichtmitglied an ein anderes zu senden.
- Die gesamte Kommunikation über das Web erfolgt verschlüsselt mit SSL .
- Der gesamte Authentifizierungsverkehr zwischen dem ZendTo Server und seinen Authentifizierern wird mit SSL verschlüsselt.
- Bei Verwendung der SQL-basierten Authentifizierung werden Benutzerkennwörter nicht gespeichert. Stattdessen wird ein Einweg-Hash der Passwörter gespeichert, der ausreicht, um Benutzer zu authentifizieren.
- Alle eingegebenen Benutzernamen werden mit einem konfigurierbaren regulären Ausdruck verglichen, wodurch LDAP-Injection-Angriffe vermieden werden.
- Alle eingegebenen E-Mail-Adressen werden gegen einen regulären Ausdruck geprüft, wodurch Angriffe auf das E-Mail-Routing durch Methoden wie "%" in einer Adresse ausgeschlossen werden.
- Alle in einem Webformular eingegebenen Werte sind so codiert, dass sie nicht-alphabetische Zeichen verarbeiten können, wodurch SQL-Injection- und HTML-Injection-Angriffe vermieden werden.
- Alle in einem Webformular eingegebenen Werte werden mit konfigurierbaren regulären Ausdrücken verglichen, um unbekannte Angriffe auszuschließen.
- Da es in PHP geschrieben ist, werden die meisten Pufferüberlaufangriffe eliminiert.

- Die Dateinamen der Benutzer werden niemals direkt im Dateispeicher verwendet, in dem alle aktuellen Dateien gespeichert sind. Sie werden alle durch zufällige Zeichenfolgen ersetzt, sodass das Durchsuchen des Dateisystems für einen Benutzer, der Zugriff auf das Dateisystem hat, nur sehr wenige nützliche Informationen liefert.
- Alle Aktivitäten werden sowohl von ZendTo als auch vom Webserver protokolliert.
- In allen E-Mail-Nachrichten an Benutzer wird deutlich hervorgehoben, dass sie dem Link in der Nachricht nur folgen müssen, wenn sie damit gerechnet haben, dass sie diese erhalten, und wenn nicht, sie vollständig zu ignorieren.
- Nicht authentifizierte Benutzer müssen durch Bestehen eines CAPTCHA-Tests nachweisen, dass sie ein Mensch und kein Computer sind.
- Nicht authentifizierte Benutzer müssen nachweisen, dass sie die E-Mail-Adresse besitzen, die sie verwenden möchten, indem sie einen Authentifizierungsschlüssel vorlegen, der ihnen per E-Mail zugesandt wird.
- Alle Authentifizierungstoken dürfen nur einmal verwendet werden, um Wiedergabeangriffe auszuschließen.
- Alle "Request for Dropoff" -Token dürfen nur einmal verwendet werden, um Wiedergabeangriffe auszuschließen.
- Wiederholte fehlgeschlagene Anmeldeversuche in einem konfigurierbaren Zeitraum führen dazu, dass der Benutzer für einen konfigurierbaren Zeitraum gesperrt wird, wodurch Brute-Force-Angriffe zum Unterbrechen von Kennwörtern vermieden werden.
- Alle hochgeladenen Dateien werden auf Viren überprüft und die gesamte Abgabe wird abgelehnt, wenn festgestellt wird, dass eine Datei infiziert ist.
- Der Ausfall des Virenscanners führt dazu, dass alle Abgaben abgelehnt werden, wodurch Angriffe ausgeschlossen werden, die versuchen, den Virenscanner zu umgehen, indem er zerstört wird

3.3 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- alle berechtigten Personen (Interne) werden namentlich (oder Alias) im System als berechtigter Empfänger hinterlegt. Die E-Mailadresse muss valide sein jedoch verweisen wir auf den Hinweis in Punkt 2.1
- Der „Interne-Nutzer“ kann zusätzlich auch Daten von einem Absender anfordern indem er diesen einen Link sendet und zur Abgabe von Daten auffordert. Diese Form der Abgabe erleichtert sich darin, dass der Absender nur die angeforderten Daten hochladen muss.
- Der berechtigte Empfänger kann auch unaufgefordert Daten empfangen, jedoch findet für den Absender eine E-Mail-Verifikation statt.

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber 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 unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber 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 Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber 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 Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber 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 Auftraggeber unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt grundsätzlich in einem deutschen Rechenzentrum mit Tüv-Zertifikat (ISO 27001). Jegliche Verlagerung in ein Drittland darf nur mit ausdrücklicher Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

5 Sicherheit der Verarbeitung

(1) Die im Anhang 1 für das Rechenzentrum und unter Punkt 3.2 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 Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

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

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

(5) Kopien oder Duplikate werden nicht erstellt. Ausgenommen ist die wunschgemäße Sicherung der Logdatei um Zugriffe auf das System lückenlos zu dokumentieren; soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) 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 Auftraggeber spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden. Nachweise sind mindestens bis zum Ablauf drei Kalenderjahren nach Beendigung der Auftragsverarbeitung aufzubewahren und dem Auftraggeber jederzeit auf Verlangen vorzulegen.

6 Regelungen zur Löschung von Daten

(1) Im Rahmen des Auftragsvereinbaren die Parteien die Dauer des Verbleibs von hochgeladenen Daten. Die Daten werden Systemseitig automatisch gelöscht, es sei denn der Empfänger löscht die Daten manuell nach seinem Download via Löschbutton.

(2) Endet der Vertrag werden alle Daten unverzüglich gelöscht. Der Datenträger/Server wird vollständig gelöscht und mit einem neuen Betriebssystem überspielt. Eine Datensicherung findet nicht statt.

7 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist unzulässig

8 Rechte und Pflichten des Auftraggebers

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

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

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

(4) Der Auftraggeber 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. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter 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 Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. eine Beschreibung der Art der Verletzung des Schutzes von Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Daten, 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 Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.
(2) Auftraggeber 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 Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber 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 Auftraggeber bestätigt oder geändert wird.
(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

(1) Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten noch in der Verfügungsgewalt des Auftragnehmers, wird dieser auf Anforderung des Auftraggebers diese unverzüglich löschen. Die Löschung findet direkt auf dem Server statt indem dieser mit einem neuen Betriebssystem überspielt wird. Datensicherungen werden während des Vertragsverhältnis sowie auch nach Vertragslösung niemals erstellt
(2) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
(3) Logdateien, (soweit diese durch den Auftraggeber gewünscht wurden) werden durch den Auftragnehmer mindestens bis zum Ablauf des dritten Kalendertages nach 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 Auftraggeber 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. Ist die Speicherfrist der Daten abgelaufen und/oder können die Originaldatei(en) nicht mehr nachvollzogen werden ist der Auftragnehmer und Auftraggeber von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber und Auftragnehmer erhoben werden.

(3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung vorsätzlich verursacht haben.

14 Vertragsstrafe

(1) Der Auftragnehmer schuldet bei schuldhaften Verstößen gegen die Abmachungen dieses Vertrages eine sofort fällige Vertragsstrafe in Höhe der monatlichen Vergütung. Die Vertragsstrafe wird insbesondere bei Mängeln in der Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen verwirkt. Bei dauerhaften Verstößen gilt jeder Kalendermonat, in dem der Verstoß ganz oder teilweise erneut vorliegt, als Einzelfall. Die Einrede des Fortsetzungszusammenhangs ist ausgeschlossen.

(2) Nutzt der Auftraggeber den Service mit strafbaren Inhalten und ist der Auftragnehmer diesbezüglich Seitens der Judikative zur Stellungnahme aufgefordert worden, unterrichtet der Auftragnehmer sogleich den Auftraggeber und nur dann stellt er eine Sicherungskopie für die Judikative her. Der Umstandsverursacher trägt hierfür die Kosten und Folgekosten aller Betreffenden in voller Höhe

15 Sonderkündigungsrecht

(1) Der Auftraggeber 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 Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers 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 Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

(4) Der Auftragnehmer hat dem Auftraggeber alle überzahlten Beträge zu erstatten.

16 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 Vertrages 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 Auftraggebers 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 Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform und die ausdrückliche Bezugnahme auf diese Vereinbarung 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.

Unterschriften

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer

Anlage 1 technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen 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.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management; inkl. der geforderten regelmäßigen Überprüfung, Bewertung und Evaluierung der Datenschutzmaßnahmen!
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 2 Zugelassene Dienstleister

Es werden keine Subunternehmen beauftragt.

Das Rechenzentrum in München (Deutschland) ist nicht als Subunternehmen beschäftigt, sondern stellt sich als Dienstleister / Rechenzentrum zur Verfügung.

Die Einhaltung der DSGVO Vorschriften sind in diesem Unternehmen zertifiziert.

Das Rechenzentrum gehört zu den sichersten weltweit. Das Rechenzentrum München hat sich freiwillig höchsten Standards in puncto Datenschutz und Datensicherheit verpflichtet – zusätzlich zu den strengen gesetzlichen Auflagen in Deutschland. In IT-Infrastrukturen sind die Daten von rund vier Millionen Internetpräsenzen und mehr als 60.000 Servern so sicher aufgehoben wie in einem Safe.

Auch der TÜV ist von der Qualität dieses Rechenzentrums überzeugt. Das RZ München trägt bereits seit 2004 das begehrte TÜV-Siegel nach ISO 27001 (ehemals 7799) für hervorragende Verfügbarkeit und IT-Sicherheit aller Cloud Services. Zudem umfasst diese Zertifizierung zahlreiche Sicherheitsmaßnahmen in der IT-Infrastruktur selbst, in der Sekundärtechnik und in der Prozesskette. Dieser Umstand wird jedes Jahr aufs Neue nach ISO 27001 geprüft und zertifiziert.

Anlage 3 Weisungsberechtigte Personen, Adresse zur Meldung von Datenschutzverletzungen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Detlef Köppel – Am Kiesgrund 34a – 16548 Glienicke Nordbahn.

In Vertretung: Heike Köppel ,jedoch nicht zur Ausführung von Anweisungen.

Die Kontaktwege des Auftraggebers werden im Hauptvertrag ausgewiesen.

Anlage 4 Datenschutzbeauftragter

Derzeit ist kein / externer Datenschutzbeauftragter beim Auftragnehmer bestellt:

Wünscht der Auftraggeber die Benennung eines Datenschutzbeauftragten wird der Auftragnehmer zeitnah die Benennung nachholen sobald eine Kostenübernahmeerklärung vorliegt soweit nicht im Hauptvertrag vereinbart.