eRecht24
PREMIUM

MUSTER

„Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 III DSGVO“

Stand: 07.02.2023

www.e-recht24.de

Wichtige Hinweise zur Benutzung des eRecht24 Premium Musters „Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 III DSGVO“

- Die leeren Felder müssen mit Ihren individuellen Angaben ausgefüllt werden.
- Die Hinweise in den eckigen Klammern dienen lediglich als Erklärung und zur Verständlichkeit des Musters. Sie gehören nicht zum Rechtstext des Vertragsmusters.
- Bitte beachten Sie, dass das Muster lediglich eine Anregung für eine betreffende Vereinbarung ist, die an Ihre spezifischen Anforderungen angepasst werden muss.
- Das Muster ist „neutral“ formuliert, so dass die Interessen von Auftraggeber und Auftragsverarbeiter berücksichtigt sind. Je nachdem ob Sie als Auftraggeber oder als Auftragsverarbeiter tätig sind, ist es sinnvoll, das Muster etwa in den Punkten Haftung, Rechte und Pflichten konkret für Auftraggeber oder Auftragsverarbeiter anzupassen.
- Das Muster gilt nur für Verträge, die mit einem Auftragsverarbeiter mit Sitz in einem Mitgliedstaat der EU oder in einem Mitgliedstaat des Europäischen Wirtschaftsraums (Island, Liechtenstein und Norwegen) abgeschlossen werden. AV-Verträge mit Unternehmen die nicht in der EU / EWR sitzen bzw. Daten dorthin übertragen und speichern erfordern eine individuelle Rechtsberatung.
- Bitte füllen Sie unbedingt die dem Vertrag beigefügten Anlagen aus. Anderenfalls ist der Vertrag unwirksam.
- Das Muster wurde zuletzt im Februar 2023 aktualisiert und auf die neuesten Anforderungen angepasst.
- Als eRecht24 Premium Mitglied dürfen Sie dieses Muster für eigene Zwecke und Verträge mit Ihren Kunden oder Dienstleistern verwenden.
- Sie dürfen das eRecht24 Premium Muster nicht verkaufen, vertreiben oder anderen kostenpflichtig oder kostenlos zur Verfügung stellen. Alle Rechte vorbehalten.
- Da die Materie sehr komplex und die Ausgangslage in fast jedem Fall eine andere ist können wir ohne individuelle Beratung und Prüfung keine Haftung übernehmen.
- Eine individuelle Beratung dazu ist auch nicht im Rahmen der eRecht24 Premium Erstberatung möglich.
- Benötigen Sie anwaltlichen Rat und Hilfe bei der Erstellung von Rechtstexten oder Verträgen? Dann lassen Sie sich von unseren Kollegen der Kanzlei Siebert Lexow unterstützen!

Mustervereinbarung zur Auftragsverarbeitung

Zwischen

.....

Bezeichnung des Unternehmens, Firma

.....

Straße, Hausnummer

.....

PLZ / Ort

nachfolgend „Auftraggeber“

und

.....

Bezeichnung des Unternehmens, Firma

.....

Straße, Hausnummer

.....

PLZ / Ort

nachfolgend „Auftragsverarbeiter“

(nachfolgend beide Parteien auch bezeichnet als „Partei“ oder „Parteien“)

§ 1 Allgemeine Bestimmungen und Auftragsgegenstand

(1) Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Verarbeitung sind Anlage 1 zu entnehmen.

(2) Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.

(3) Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.

(4) Die Vergütung wird außerhalb dieses Vertrags vereinbart.

§ 2 Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

§ 3 Weisungen des Auftraggebers

(1) Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

(2) Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

(3) Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

(4) Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

§ 4 Kontrollbefugnisse

(1) Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen.

(2) Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlauffrist erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.

(3) Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

§ 5 Allgemeine Pflichten des Auftragsverarbeiters

(1) Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur zulässig, wenn der Auftragnehmer nach dem Recht der Europäischen Union oder der Mitgliedstaaten zur Datenverarbeitung verpflichtet ist. Im Falle einer solchen Verarbeitung, informiert der Auftragnehmer den Auftraggeber unverzüglich über beabsichtigte oder bereits eingeleitete Verarbeitung, es sei denn, dass das betreffende Recht der Europäischen Union oder des Mitgliedstaates eine solche Mitteilung aufgrund eines wichtigen öffentlichen Interesses verbietet; in diesem Fall erfolgt die Mitteilung unverzüglich, sobald die rechtlichen Hindernisse nicht mehr bestehen.

(2) Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen zu implementieren .

(3) Sofern der Auftragsverarbeiter nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

(4) Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice des Auftragsverarbeiters) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

(5) Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

(6) Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.

(2) Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

§ 7 Unterstützungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

(2) Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

§ 8 Einsatz von Unterauftragsverarbeitung (Subunternehmer)

(1) Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragsverarbeiters sind diesem Vertrag abschließend in Anlage 3 beigefügt. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als

erteilt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden.

(2) Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragsverarbeiter wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

(3) Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können.

(4) Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. dem Subunternehmer zur Ausübung der gleichen Kontrollrechte, wie ggü. dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.

(5) Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO ggü. den ihm unterstellten Personen erfüllt hat.

(6) Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.

(7) Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.

(8) Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

§ 9 Mitteilungspflichten des Auftragsverarbeiters

(1) Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

(2) Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.

(3) Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

(4) Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle

Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

§ 10 Vertragsbedingung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

§ 11 Datengeheimnis und Vertraulichkeit

(1) Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich und im Einklang mit den Vorgaben der DSGVO und der sonstigen Datenschutzgesetze zu behandeln.

(2) Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.

(3) Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

§ 12 Schlussbestimmungen

(1) Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

(2) Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

(4) Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

.....

Ort, Datum Unterschrift Auftraggeber

.....

Ort, Datum Unterschrift Auftragsverarbeiter

Anlage 1 – Auftragsdetails

Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:
[Hier müssen sämtliche Leistungen im Rahmen der Verarbeitung personenbezogener Daten benannt werden.]

.....
.....
.....
.....
.....
.....

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:
[Hier muss eine detaillierte Aufstellung der verarbeiteten Datenarten erfolgen (z.B.: Daten von Bürgern, Name, Vorname, Anschrift Geburtsdatum, Beruf, etc.]

.....
.....
.....
.....
.....
.....

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:
[Auflistung der betroffenen Personengruppen; vorliegend z.B. Mitarbeiter, Kunden, etc.]

.....
.....
.....
.....
.....
.....

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

I. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System
- Trennung von Produktiv- und Testsystem
- Sonstige:

  .....
  .....

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

(1) Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

.....
.....
.....
(Bitte Verschlüsselungs-Maßnahmen konkret beschreiben)

(2) Pseudonymisierung

„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

( ) Nein.
( ) Ja, und zwar in folgender Art und Weise:

.....
.....
.....
(Bitte Maßnahmen zur Pseudonymisierung konkret beschreiben)

(3) Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern (Zutrittskontrolle):

- Alarmanlage
- Absicherung von Gebäudeschächten
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Schließsystem mit Codesperre
- Manuelles Schließsystem
- Biometrische Zugangssperren
- Videoüberwachung der Zugänge
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen
- Zutrittskonzept / Besucherregelung
- Sonstige:

.....
.....
.....

(4) Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern (Zugangskontrolle):

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
- Authentifikation mit biometrischen Verfahren
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Gehäuseverriegelungen
- Einsatz von VPN-Technologie bei der Übertragung von Daten
- Verschlüsselung mobiler IT-Systeme
- Verschlüsselung mobiler Datenträger
- Verschlüsselung der Datensicherungssysteme
- Sperren externer Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Sonstige:

.....
.....
.....
.....

(5) Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern
- Sonstige:

.....
.....
.....

(6) Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

- Sonstige:

.....
.....

(7) Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die von Unterauftragnehmern / Subunternehmern des Auftragnehmers verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und des Auftragnehmers verarbeitet werden können (Auftragskontrolle).

- Auswahl des Subunternehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung der und Dokumentation der beim Subunternehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Subunternehmer (z.B. durch Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Subunternehmers auf das Datengeheimnis
- Subunternehmer hat Datenschutzbeauftragten bestellt
- Sicherstellung der Vernichtung von Daten von den Systemen des Subunternehmers nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Subunternehmer vereinbart
- laufende Überprüfung des Subunternehmers und seiner Tätigkeiten
- Vertragsstrafen bei Verstößen
- Sonstige:

.....
.....
.....

(8) Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können (Transport- bzw. Weitergabekontrolle):

- Einsatz von VPN-Tunneln
- Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E-Mail-Verkehrs)
- Verschlüsselung physischer Datenträger bei Transport
- Sonstiges:

.....
.....
.....

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimatisierung der Serverräume
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- In Hochwassergebieten: Serverräume über der Wassergrenze
- belastbares Datensicherungs- und Widerherstellungskonzept vorhanden
- Sonstige:

.....
.....
.....

IV. Besondere Datenschutzmaßnahmen

Es liegen schriftlich vor:

- interne Verhaltensregeln
- Risikoanalyse
- Datenschutz-Folgenabschätzung
- Datensicherheitskonzept
- Wiederanlaufkonzept
- Zertifikat:

  .....

- Sonstiges:

  .....
  .....
  .....

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von ..... Monaten / Jahren und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

[Diese Seite kann bei einer längeren Liste von aufzuführenden Subunternehmen beliebig oft kopiert und ausgefüllt werden.]

(Unternehmens-) Name und Anschrift

.....
.....

Beschreibung der Leistung

.....
.....
.....

Ort der Leistung

.....

(Unternehmens-) Name und Anschrift

.....
.....

Beschreibung der Leistung

.....
.....
.....

Ort der Leistung

.....

eRecht24 PREMIUM

Schnell und einfach zur rechtssicheren Website mit eRecht24 Premium

Schritt für Schritt zur rechtssicheren Website

Mit dem Projekt Manager & Planer schnell und einfach Rechtstexte für Ihre Webseiten erstellen und automatisiert aktualisieren

Antworten auf Ihre Fragen vom Profi

Für die kostenlose Erstberatung zum Internetrecht & Datenschutz steht Ihnen das Kanzlei-Team Siebert Lexow jederzeit zur Verfügung

Premium-Memberbereich mit exklusiven Inhalten

Profitieren Sie von einer Vielzahl exklusiver Live-Webinare, praktischen Checklisten und Mustern für Ihre Webprojekte

Nichts mehr vergessen und immer auf der sicheren Seite

Planen, erstellen und aktualisieren Sie Ihre Projekte und Webseiten ohne jemals wieder etwas zu vergessen

Professionelle Beratung ohne versteckte Kosten

Erstberatung ohne lange Wartezeiten – alle Antworten auf Ihre Fragen finden Sie kostenfrei in der Erstberatung

Endlich verständliches Know How zum Internetrecht

Alle Inhalte bei eRecht24 Premium sind praktisch und verständlich aufbereitet und helfen Ihnen bei Ihrer täglichen Arbeit an Ihren Webseiten

Über 60.000 zufriedene Kunden

+ 1 Million
Angelegte Impressumstexte

465.810
Mit Premium abgesicherte Webprojekte

96%
Weiter-empfehlungsrate

Quelle: eRecht24 Premium Zufriedenheitsumfrage 05/2020 - 06/2020

JETZT MITGLIED WERDEN

www.e-recht24.de/mitglieder

eRecht24 GmbH & Co. KG, Lietzenburger Straße 94, 10719 Berlin
Rechtsanwalt Sören Siebert & Dipl.-Wirtsch.-Inf. Karsten Fernkorn
E-Mail: support@e-recht24.de Telefon: 030-12088634
UST-ID: DE242329852