#Datenschutzrechtliche Vereinbarung

(nachfolgend auch Vertrag genannt) über die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung gemäß Art. 28 DS-GVO)

Zwischen

Dem Kunden

- „Auftraggeber“ -

und

Gender-API.com
Markus Perl IT Solutions
Hermann-Mayrhofer-Str. 3
94036 Passau

- „Auftragsverarbeiter“ -

1. Gegenstand und Dauer der Vereinbarung

Die folgenden Dienstleistungen werden in Auftrag gegeben: Operative Verarbeitung personenbezogener Daten im Rahmen der Erbringung der vereinbarten Dienstleistung.

Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags: Die Vertragslaufzeit richtet sich nach dem Hauptvertrag (Allgemeinen Geschäftsbedingungen https://gender-api.com/de/terms-of-use).

2. Zweck, Umfang und Art der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Die Verarbeitung personenbezogener Daten im Auftrag erfolgt ausschließlich zweckgebunden. Der Zweck, der Umfang und die Art sind wie folgt (gemäß der Definition von Art. 4 Nr. 2 DS-GVO): Der Gegenstand des Auftrags ergibt sich aus den vom Auftraggeber ausgewählten Leistungen („Paketen“) auf der Internetseite Gender-API.com. Dabei handelt es sich um SaaS-Lösungen zur Geschlechtsbestimmung und Aufbereitung von personenbezogenen Daten (software as a service). Diese Leistungen werden entweder sofort über eine API Schnittstelle oder im Falle der Massenbearbeitung als Batch-Vorgang über eine verschlüsselte Schnittstellen erbracht.

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO): * Customers, Leads, Vendors

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO):

- Personenstammdaten
- Kommunikationsdaten (z.B. E-Mail)
- Vertragsstammdaten
- Protokolldaten
- Auftraggeber Login und Profil-Daten
- API Schnittstelle: Anrede, Vorname, Nachname, E-Mail, Land, E-Mail Adresse, IP Adresse, Locale von durch den Auftraggeber bereitgstelleten Daten
- Massenbearbeitung als Batch-Vorgang: Anrede, Vorname, Nachname, E-Mail, Land, E-Mail Adresse, IP Adresse, Locale von durch den Auftraggeber bereitgstelleten Daten

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragsverarbeiter abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragsverarbeiters

Weisungsberechtigte Funktionen des Auftraggebers sind: 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. 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. Weisungsempfänger beim Auftragsverarbeiter sind: Hier wird der beim Auftragsverarbeiter festgelegte Weisungsempfänger (Person oder Funktion) eingetragen. 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. Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen. Für Weisung zu nutzende Kommunikationskanäle:

- postalisch an folgende Anschrift: Markus Perl IT Solutions – Gender-API.com, Hermann-Mayrhofer-Str. 3, 94036 Passau.
- per Email an folgende Adresse: contact@gender-api.com.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner

unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen/Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO). Der Auftragsverarbeiter verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Der Auftragsverarbeiter hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

- Verfügbarkeitskontrolle der Daten durch mindestens tägliche Datensicherung
- Plausibilitätskontrolle der Verarbeitungsergebnisse

Das Ergebnis der Kontrollen ist zu dokumentieren.

Processor must cooperate to the extent necessary and adequately assist Controller as much as possible in fulfilling the rights of the data subjects per Art. 12 to 22 GDPR, preparing directories of processing activities and conducting the required data protection impact assessments (Article 28 (3) sentence 2 (e) and (f) GDPR). Processor must forward all information required for these purposes immediately to the following parties at the Controller: The authorized instruction giver named in section 4. Der Auftragsverarbeiter muss im erforderlichen Umfang kooperieren und den Auftraggeber so weit wie möglich bei der Erfüllung der Rechte der betroffenen Personen gemäß Art. 12 bis 22 BPR, bei der Erstellung von Verzeichnissen der Verarbeitungstätigkeiten und bei der Durchführung der erforderlichen Datenschutzfolgenabschätzungen (Art. 28 Abs. 3 Satz 2 Bst. e und f DSGVO) unterstützen. Der Bearbeiter muss alle für diese Zwecke erforderlichen Informationen unverzüglich an die folgenden Parteien beim Auftraggeber weiterleiten: Den in Ziffer 4 genannte Weisungsberechtigten.

Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird. Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen. Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der Auftragsverarbeiter sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit/Home Office von Beschäftigten des Auftragsverarbeiters) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen. Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutz-rechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen:

- Telekommunikationsgeheimnis nach dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG)

Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragsverarbeiter ist als Beauftragte(r) für den Datenschutz bestellt:

Dr. Sebastian Kraska
IITR Datenschutz GmbH, Marienplatz 2, 80331 München
+49 89 1891 7360
email@iitr.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragsverarbeiter sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern für Kerndienstleistungen (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die zukünftige Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragsverarbeiter ohne gesonderte Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DS-GVO. Der Auftragsverarbeiter muss dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen zudem immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragsverarbeiter auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragsverarbeiters und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO). Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die

Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat. Der Auftragsverarbeiter hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen: Regelmäßige Prüfung der beim Subunternehmer eingerichteten technischen und organisatorischen Maßnahmen (mindestens alle 2 Jahre) mittels eines Fragenkataloges Regelmäßige Prüfung der beim Subunternehmer eingerichteten Datenschutzkonzeptes (mindestens alle 2 Jahre)

Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen. Der Auftragsverarbeiter haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragsverarbeiter im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden. Zurzeit sind für den Auftragsverarbeiter Dies muss der Auftragsverarbeiter ankreuzen, wenn er Subunternehmer im Zusammenhang mit der Verarbeitung personenbezogener Daten des Auftraggebers einsetzt. Die Subunternehmer müssen dann vom Auftragsverarbeiter in der Anlage 1 mit der kompletten Anschrift genannt werden. die in der Anlage 1 dokumentierten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit der Beauftragung der in Anlage 1 genannten Subunternehmer erklärt sich der Auftraggeber einverstanden. Dies muss der Auftragsverarbeiter ankreuzen, wenn er keine Subunternehmer im Zusammenhang mit der Verarbeitung personenbezogener Daten des Auftraggebers einsetzt. keine Subunternehmer beschäftigt. Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer. Der Auftraggeber erhält die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben, sofern die bisher vereinbarten und von Auftragsverarbeiter zugesicherten technischen und organisatorischen Maßnahmen nicht vollständig gewährleistet werden können (§ 28 Abs. 2 Satz 2 DS-GVO). In diesem Fall darf die beabsichtigte Änderung nicht vollzogen werden.

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine angemessene und nachvollziehbare Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen berücksichtigt.

Das in Anlage 2 beschriebene Datenschutzkonzept stellt die Mindestanforderungen der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter dar. Hierbei ist auch das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung beschrieben.

Folgende Möglichkeiten für den Nachweis durch Zertifizierung bestehen: Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragsverarbeiter und Auftraggeber abzustimmen. Soweit die beim Auftragsverarbeiter getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Die Maßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragsverarbeiter mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragsverarbeiters nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

- Maschinelle Löschung, nach einem fest definierten und versioniertem Algorithmus

10. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Als Gerichtsstand wird das für den Auftraggeber örtlich zuständige Gericht vereinbart. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich zu verständigen. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anlage 1 - Unterauftragsverhältnisse

Aktuell bestehen die nachfolgenden Unterauftragsverhältnisse im Zusammenhang mit der Auftragsverarbeitung: https://gender-api.com/en/privacy-policy/subcontractors

Anlage 2 – Technische und organisatorische Maßnahmen / Datenschutzkonzept

Der Auftragsverarbeiter sichert zu, dass er die nachfolgend beschriebenen Mindestanforderungen im Rahmen seines Datenschutzkonzeptes einhält. Es beschreibt die im Rahmen der Auftragsverarbeitung erforderlichen Maßnahmen beim Auftragsverarbeiter zum sicheren Umgang mit personenbezogenen Daten. Die Grundlage für dieses Datenschutz-Konzept bilden die EU-Datenschutzgrundverordnung DS-GVO und ggf. weitere von den interessierten Parteien geforderten Maßnahmen. Hierbei orientiert sich der Auftragsverarbeiter im Wesentlichen an den Vorgaben der Artikel 24, 25 und 32 DS-GVO. Auf Anforderung weist der Auftragsverarbeiter die Einhaltung entsprechend nach.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Die Räume, in denen die Verarbeitung personenbezogener Daten erfolgt oder Datenverarbeitungsanlagen installiert sind, dürfen nicht frei zugänglich sein. Sie müssen bei Abwesenheit der Mitarbeiter verschlossen sein. Die Zutrittsberechtigungen müssen in einem geregelten Verfahren nach dem „Need-to-know-Prinzip“ vergeben und regelmäßig hinsichtlich ihrer Erforderlichkeit überwacht werden. Räume, in denen Datenverarbeitungsanlagen (Rechenzentrum, Server, Netzwerkverteiler usw.) untergebracht sind, müssen besonders zutrittsgeschützt sein und dürfen nur für Beschäftigte der IT-Administration (ggfs. der Geschäftsleitung) zugänglich sein. Alternativ müssen die Geräte in geeigneten und verschlossenen Schränken untergebracht sein. Besucher und unternehmensfremde Personen müssen in einem dokumentierten Verfahren registriert und innerhalb der Geschäftsräume beaufsichtigt werden.

1.2. Zugangskontrolle

Für jeden Netzwerkbenutzer muss ein persönlich zugeordneter Benutzer mit einem mindestens 10-stelligen Passwort mit Groß- und Kleinbuchstaben, Ziffer und Sonderzeichen eingerichtet sein. Die Nutzer sind systemseitig zu verpflichten, die Passwörter mindestens alle 90 Tage zu verändern. Die Netzwerkbenutzer sind auf die Einhaltung der Benutzerzugangsrichtlinie dokumentiert zu verpflichten. Die Einrichtung, Änderung und der Entzug von Zugangsberechtigungen müssen in einem dokumentierten Verfahren erfolgen. Eingerichtete Zugangsberechtigungen müssen regelmäßig hinsichtlich ihrer Erforderlichkeit dokumentiert überprüft werden. Die Netzwerkzugriffe müssen überwacht und protokolliert werden, dies beinhaltet auch nicht erfolgreiche Anmeldeversuche.

1.3 Zugriffskontrolle

Für die Zugriffe auf personenbezogene Daten muss ein dokumentiertes, rollenbasiertes Berechtigungskonzept vorhanden sein, welches die Zugriffe in der Form einschränkt, dass nur berechtigte Personen auf die für ihre Aufgabe notwendigen personenbezogenen Daten zugreifen können (Minimumprinzip). Die Passwort-Regelungen aus der Zugangskontrolle müssen auch im Rahmen der Zugriffskontrolle umgesetzt werden. Die administrativen Tätigkeiten müssen auf einen kleinen Kreis von Administratoren eingeschränkt sein. Die Tätigkeiten der Administratoren müssen im Rahmen technisch vertretbaren Aufwandes überwacht und protokolliert werden.

1.4 Pseudonymisierung

Auswertungen müssen pseudonymisiert werden, sofern der Personenbezug für das Ergebnis nicht zwingend erforderlich ist.

1.5 Trennungskontrolle

Die Trennung von personenbezogenen Daten muss durch unterschiedliche Speicherorte oder durch eine Mandantentrennung sichergestellt werden.

2. Integrität

2.1 Weitergabekontrolle

Im Rahmen der Weitergabekontrolle muss sichergestellt werden, dass nur berechtigte Personen die personenbezogenen Daten zur Kenntnis nehmen können. Bei einer Übermittlung per E-Mail sind entsprechende Schutzmaßnahmen (z.B. Verschlüsselung der Kommunikation zwischen den Mail-Servern) zu ergreifen. Mobile Geräte oder mobile Speichermedien müssen verschlüsselt werden, wenn auf ihnen personenbezogene Daten gespeichert werden.

2.2 Eingabekontrolle

Die Eingabe, Änderung und Löschung personenbezogener Daten muss dem durchführenden Beschäftigten zugeordnet werden können. Die Änderung und Löschungen von Datensätzen muss systemseitig eingeschränkt sein, damit ein versehentliches Ändern oder Löschen wirksam verhindert wird.

2.3 Auftragskontrolle

Im Rahmen der Auftragskontrolle muss sichergestellt werden, dass die im Auftrag durchgeführten Datenverarbeitungsvorgänge ausschließlich auf Weisung des Auftraggebers erfolgen. Hierzu müssen die mit der Datenverarbeitung Beschäftigten geschult und unterwiesen werden. Die Auftragsverarbeitung muss durch interne Kontrollen überwacht werden. Die Ergebnisse der Kontrollen müssen dokumentiert werden. Unterauftragnehmer dürfen nur auf Basis der mit dem Auftraggeber vereinbarten Regelungen beauftragt werden. Die Übermittlung oder der Zugriff auf personenbezogene Daten darf erst dann erfolgen, wenn der Unterauftragnehmer eine Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO unterzeichnet hat und die Einhaltung der Regelungen des Datenschutzkonzeptes bestätigt hat. Die Prüfpflicht des Auftragnehmers gegenüber seinem Unterauftragnehmer ergibt sich aus der mit dem Auftraggeber abgeschlossenen Vereinbarung zur Auftragsverarbeitung.

3. Verfügbarkeit und Belastbarkeit

Die Verarbeitung von personenbezogenen Daten muss auf Datenverarbeitungssystemen erfolgen, die einem regelmäßigen und dokumentierten Patch-Management unterliegen. Es dürfen im Netz keine Systeme verbunden sein, die außerhalb der Wartungszyklen der Hersteller sind (insb. kein Windows XP, Windows Server 2003 etc.). Sicherheitsrelevante Patches müssen innerhalb von 72 Stunden nach Bekanntgabe eingespielt werden. Die durchgängige Verfügbarkeit von personenbezogenen Daten muss mittels redundanten Speichermedien und Datensicherungen gemäß dem Stand der Technik gewährleistet werden. Rechenzentren und Serverräume müssen dem Stand der Technik (Temperaturregelung, Brandschutz, Wassereinbruch etc.) entsprechen. Die Server müssen über eine unterbrechungsfreie Stromversorgung (USV) verfügen, die ein geregeltes Herunterfahren ohne Datenverlust sicherstellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es muss ein Verfahren zur Überwachung des Datenschutzes im Unternehmen implementiert sein. Dieses muss die Verpflichtung der Beschäftigten auf das Datengeheimnis, die Schulung und Sensibilisierung der Beschäftigten und die regemäßige Auditierung der Datenverarbeitungsverfahren beinhaltet. Ebenso muss die Dokumentation des für den Auftraggeber durchgeführten Verarbeitungsverfahrens vor Aufnahme der Datenverarbeitung erfolgen. Für Datenschutzverletzungen und die Wahrung der Betroffenenrechte muss ein durchgängiger Meldeprozess und Bearbeitungsprozess eingeführt sein. Dieser muss auch die Information des Auftraggebers beinhalten.