

World4You Auftragsverarbeitungsvertrag (AVV - nach Art. 28 Abs. 3 Datenschutz-Grundverordnung)

1. Gegenstand und Dauer der Verarbeitung

1.1 Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Leistungsbeschreibung und AGB (nachfolgend Hauptvertrag), soweit eine Verarbeitung von personenbezogenen Daten durch World4You (nachfolgend Auftragnehmer) als Auftragsverarbeiter für den Kunden als Verantwortlicher (nachfolgend Auftraggeber) gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

1.2 Die Dauer der Verarbeitung entspricht der im Vertrag vereinbarten Laufzeit.

2. Art und Zweck der Verarbeitung

2.1 Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags.

2.2 Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung (siehe hierzu auch Anhang 1 Leistungsbeschreibung), insbesondere im Bereich Cloud-Dienstleistungen, Hosting, Software as a Service (SaaS) und IT-Support, erforderlichen Zwecke.

3. Art der personenbezogenen Daten und Kategorien von Betroffenen

3.1 Die Art der verarbeiteten Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten. Siehe hierzu auch die Leistungsbeschreibung Anhang 1.

3.2 Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten. Siehe hierzu auch die Leistungsbeschreibung Anhang 1.

4. Verantwortlichkeit und Verarbeitung auf dokumentierte Weisungen

4.1 Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung

allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung.

4.2 Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden. Eine Unzumutbarkeit liegt insbesondere vor, wenn die Leistungen in einer Infrastruktur erbracht werden, die von mehreren Auftraggebern / Kunden des Auftragnehmers genutzt wird (Shared Services), und eine Änderung der Verarbeitung für einzelne Auftraggeber nicht möglich oder nicht zumutbar ist.

4.3 Die vertraglich vereinbarte Datenverarbeitung findet in der Regel überwiegend in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern nicht zur Erbringung der Leistung der Datentransfer in Drittstaaten erforderlich wird. Für den Fall, dass eine Übermittlung in einen Drittstaat erfolgt, stellt der Auftragnehmer sicher, dass die Voraussetzungen nach Art. 44 ff. DSGVO erfüllt sind.

5. Rechte des Auftraggebers, Pflichten des Auftragnehmers

5.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor (Verpflichtung nach dem Recht der Europäischen Union oder eines Mitgliedstaates). Dies bezieht sich auch auf Übermittlungen von personenbezogenen Daten an Drittländer oder internationale Organisationen. Besteht eine Verarbeitungspflicht entgegen einer Weisung, so informiert der Auftragnehmer vor der Verarbeitung den Auftraggeber über die entsprechende rechtliche Anforderung, es sei denn, das betreffende Recht verbietet eine solche Information wegen eines wichtigen öffentlichen Interesses. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Die Weisungen sind durch den Auftraggeber zu dokumentieren und mindestens für die Dauer des Auftragsverhältnisses aufzubewahren.

5.2 Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Ansprüche der betroffenen Personen nach Kapitel III der DSGVO. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen, soweit die Unterstützung nicht aufgrund eines Gesetzes- oder Vertragsverstoßes durch den

Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

5.3 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen, soweit die Unterstützung nicht aufgrund eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

5.4 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5.5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

5.6 Der Auftragnehmer gewährleistet die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Eine Kontaktmöglichkeit wird auf der Webseite des Auftragnehmers veröffentlicht.

5.7 Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Auftraggeber zurück, sofern nicht nach dem Unionsrecht oder nach dem anwendbaren Recht eines Mitgliedstaates eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart. Wählt der Auftraggeber die Rückgabe, kann der Auftragnehmer eine angemessene Vergütung verlangen. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

5.8 Machen betroffene Personen Schadensersatzansprüche nach Art. 82 DSGVO geltend, unterstützt der Auftragnehmer den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten. Der Auftragnehmer kann hierfür eine angemessene Vergütung verlangen.

6. Pflichten des Auftraggebers

6.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Durchführung des Auftrags Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

6.2 Im Falle der Beendigung verpflichtet sich der Auftraggeber, diejenigen personenbezogenen Daten vor Vertragsbeendigung zu löschen, die er in den Diensten gespeichert hat.

6.3 Auf Anforderung des Auftragnehmers benennt der Auftraggeber einen Ansprechpartner in Datenschutzangelegenheiten.

7. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8. Maßnahmen zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO

8.1 Der Auftragnehmer ergreift in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und den Schutz für die Rechte und Freiheiten der betroffenen Person gewährleistet. Der Auftraggeber ergreift in seinem Verantwortungsbereich gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

8.2 Die aktuellen technischen und organisatorischen Maßnahmen des Auftragnehmers sind unter diesem Link einsehbar. Der Auftragnehmer stellt klar, dass es sich bei den unter dem Link aufgeführten technischen und organisatorischen Maßnahmen lediglich um Beschreibungen technischer Art handelt, welche nicht als Bestandteil dieser Vereinbarung anzusehen sind.

8.3 Der Auftragnehmer betreibt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d) DSGVO.

8.4 Der Auftragnehmer passt die getroffenen Maßnahmen im Laufe der Zeit an die Entwicklungen beim Stand der Technik und die Risikolage an. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das Schutzniveau nach Art 32 DSGVO nicht unterschritten wird.

9. Nachweis und Überprüfung

9.1 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Sollte im Einzelfall

eine Inspektion beim Auftragnehmer erforderlich sein sollte, wird diese auf Kosten des Auftraggebers durch einen unabhängigen externen Prüfer durchgeführt, den der Auftragnehmer benennt. Der Auftragnehmer darf nur solche Prüfer benennen, die gegenüber dem Auftraggeber ihre Unabhängigkeit vom Auftragnehmer versichert und sich zur Verschwiegenheit verpflichtet haben.

9.4 Für Informationen und Unterstützungshandlungen kann der Auftragnehmer eine angemessene Vergütung verlangen, soweit die Kontrolle nicht wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

10. Subunternehmer (weitere Auftragsverarbeiter)

10.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.

10.2 Die aktuell eingesetzten weiteren Auftragsverarbeiter sind in Anhang 2 aufgeführt. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.

10.3 Der Auftragnehmer stellt die jeweils aktuellen Auftragsverarbeiter auf folgender Website dar: **Auftragsverarbeiter**. Der Auftraggeber hat somit die Möglichkeit, sich durch Abruf der Website über jeweils weitere Auftragsverarbeiter zu informieren.

10.4 Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem sachlichen Grund innerhalb von 14 Tagen nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer erhoben werden. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist (mindestens 14 Tage) nach Zugang des Einspruchs einstellen.

10.5 Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen. Der Auftragnehmer stellt insbesondere durch regelmäßige Überprüfungen sicher, dass die weiteren Auftragsverarbeiter die technischen und organisatorischen Maßnahmen einhalten.

11. Haftung und Schadensersatz

11.1. Im Fall der Geltendmachung eines Schadensersatzanspruches durch eine betroffene Person nach Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.

11.2. Die zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung zur Auftragsverarbeitung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter nach Art 82 DSGVO, außer soweit ausdrücklich etwas anderes vereinbart ist.

12. Vertragslaufzeit, Sonstiges

12.1 Die Vereinbarung beginnt mit dem Abschluss durch den Auftraggeber. Sie endet mit Ende des letzten Vertrages unter der jeweiligen Kundennummer. Sollte eine Auftragsverarbeitung noch nach Beendigung dieses Vertrages stattfinden, gelten die Regelungen dieser Vereinbarungen bis zum tatsächlichen Ende der Verarbeitung.

12.2 Der Auftragnehmer kann die Vereinbarung nach billigem Ermessen mit angemessener Ankündigungsfrist ändern. Insbesondere behält er sich ausdrücklich vor, die vorliegende Vereinbarung einseitig zu ändern, sofern sich wesentliche rechtliche Änderungen im Bezug auf diese Vereinbarung ergeben. Der Auftragnehmer wird den Auftraggeber über die Bedeutung der geplanten Änderung gesondert hinweisen und darüber hinaus dem Auftraggeber eine angemessene Frist zur Erklärung eines Widerspruchs einräumen. Der Auftragnehmer weist den Auftraggeber in der Änderungs-Ankündigung darauf hin, dass die Änderung wirksam wird, wenn er nicht binnen der gesetzten Frist widerspricht. Im Falle eines Widerspruchs durch den Auftraggeber steht dem Auftragnehmer ein außerordentliches Kündigungsrecht zu.

12.3 Der Auftraggeber erkennt diese Vereinbarung als Teil der AGB über die/das von ihm gebuchte/n Produkt/e an. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht.

12.4 Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragnehmers. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes. Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Österreich.

12.5 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der DSGVO liegen.

Anhang 1 zum World4You Auftragsverarbeitungsvertrag - Leistungsbeschreibung

Domain Leistungsbeschreibung:

Wenn Sie bei uns eine Domain bestellen, kümmern wir uns um die Konnektierung und die Registrierung Ihrer Domain bei der zuständigen Registry. Zudem ist die Aufrechterhaltung der Registrierung, Domainumzüge und Abmeldung Vertragsbestandteil. Gleiches gilt für auf ihren Domains basierenden SSL Zertifikaten.

Art der personenbezogenen Daten: Domain, Stammdaten (Name, Adresse, E-Mail, Telefonnummer)

Kategorien betroffener Personen: Kunden

Mail Leistungsbeschreibung:

Wenn Sie bei uns ein Mailprodukt bestellen, erhalten Sie eine oder mehrere E-Mail-Adressen. Wir legen für Sie die entsprechenden Postfächer an, auf die Sie mittels Web zugreifen oder die Sie in verschiedene Clients einbinden können. Des Weiteren können Sie im Web-Client entsprechend der gebuchten Leistung Termine und Aufgaben erstellen und Kontakte verwalten. Zudem gehört auch ein konfigurierbarer Spamfilter zum Produkt.

Art der personenbezogenen Daten: Mails, Kontakte, Termine, Domain

Kategorien betroffener Personen: Mitarbeiter

Cloud Speicher Leistungsbeschreibung:

Unser Cloud-Speicher World4You-Cloud ermöglicht die Speicherung Ihrer Daten in unserem Rechenzentrum, sodass Sie von überall und jederzeit auf die Daten zugreifen können. Sie können Freigaben auf bestimmte Ordner erteilen und diese verwalten.

Art der personenbezogene Daten: Daten, die Sie in der Cloud speichern

Kategorien betroffener Personen: Mitarbeiter

Hosting Leistungsbeschreibung:

Wenn Sie bei uns ein Hosting Paket bestellen, gehören zu unserer Leistung die Registrierung und Konnektierung der Domain sowie die Zurverfügungstellung des Webspaces und der Datenbanken. Inbegriffene Leistungen sind SSL-Zertifikate und Mail. Mittels SSL-Zertifikat werden die Daten zwischen Ihrer Webseite und dem Webserver verschlüsselt übertragen. Mit den Easy.Install Apps können Sie verschiedene Applikationen zum Aufbau und zur Verwaltung von Websites verwenden. Zusätzlich erhalten Sie Zugriff auf das Tool marketingRadar, mit dem Sie die Sichtbarkeit und das Ranking Ihrer Website bei Suchmaschinen prüfen und optimieren können.

Art der personenbezogenen Daten: Inhaltsdaten der Webseite, Domain, Daten E-Mail (siehe unter Mailprodukt), Daten Ihrer Websitebesucher
Kategorien betroffener Personen: Mitarbeiter, Besucher der Webseite

WordPress- & WooCommerce Hosting

Wenn Sie eines unserer Webhosting Pakete, die speziell auf die Verwendung für das CMS WordPress bzw WordPress mit dem WooCommerce Plug-In ausgerichtet sind, bestellen, erhalten Sie die Registrierung und Konnektierung der Domain, sowie die Zurverfügungstellung des Webspace mit direkt installierten Datenbanken für WordPress bzw WordPress inklusive WooCommerce. Zusätzlich enthalten sind SSL-Zertifikate, die Daten zwischen Ihrer Website und dem Webserver verschlüsselt übertragen, das Online-Marketing-Tool marketingRadar, mehrere E-Mail-Adressen mit entsprechenden Postfächern und Zugriff auf die World4You Cloud.

Art der personenbezogenen Daten: Inhaltsdaten der Webseite, Domain, Daten E-Mail (siehe unter Mailprodukt), Daten Ihrer Websitebesucher
Kategorien betroffener Personen: Mitarbeiter, Besucher der Webseite

Server Leistungsbeschreibung:

Sie können virtuelle Server bei uns bestellen. Wir stellen Ihnen hierfür einen geteilten Speicherplatz auf einem Server zur Verfügung.

Art der verarbeiteten Daten: Daten, die Sie auf dem Server speichern
Kategorien betroffener Personen: Mitarbeiter, Besucher der Webseite

weitere SaaS Produkte:

Wir bieten zudem noch weitere Software-as-a-Service Produkte an. Hierzu gehören z.B. - aber nicht abschließend - Online Marketing Tools, die Möglichkeit, sich eine Webseite mittels Homepage-Baukastens zu erstellen oder auch der Vertrieb von Office Anwendungen.

Art der verarbeiteten Daten: Daten, die Sie in den Diensten speichern
Kategorien betroffener Personen: Mitarbeiter, Kunden, Besucher der Webseite

Anhang 2 zum World4You Auftragsverarbeitungsvertrag - genehmigte Subunternehmen

World4You setzt folgende Subunternehmen ein:

Nr.	Name, vollständige Anschrift	Produkt / Beschreibung der Leistung
1	rankingCoachGmbH, im Mediapark 6b 50670 Köln, Deutschland	Suchmaschinenoptimierung rankingCoach Optimierung der Suchergebnisse Ihrer Website bei Google
2	IONOS SE Elgendorfer Str. 57 56410 Montabaur Deutschland	vServer, Security Dienstleistungen AD-Server
3	Google Cloud EMEA Limited Velasco Clanwilliam Place Dublin 2 Ireland	World4You Kollaborations Tools
4	Microsoft Ireland Operations Ltd One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Ireland	Security Dienstleistungen, Office Software
5	CM4all GmbH Im Mediapark 6a 50670 Köln Deutschland	Baukastensystem
6	Dixa ApS Vimmelskaflet 41 A, 1st floor 1161 Copenhagen K Dänemark	Kundenservice-Dienstleister im Bereich Telefonie, E-Mail/Ticket, Chatbot und Livechat
7	united-domains GmbH Gautinger Straße 10 82319 Starnberg Deutschland	Produktmanagement-Dienstleister (Entwicklung, Verbesserung und Verwaltung des Produktportfolios der World4You)

- | | | |
|---|---|---|
| 8 | Arsys Internet S.L.U.
C. Madre de Dios, 21
26004 Logroño
La Rioja, Spanien | Technical Operations-Dienstleister
(Setup und Wartung von Kundenservices &
internen Service-Landschaften) |
|---|---|---|

Technisch organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind. Festlegung von Sicherheitsbereichen

- Realisierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Begleitung von Fremdpersonal
- Überwachung der Räume

1.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Festlegung des Schutzbedarfs
- Zugangsschutz
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Umsetzung einfacher Authentisierung per Username/Passwort
- Protokollierung des Zugangs
- Monitoring bei kritischen IT-Systemen
- Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
- Festlegung befugter Personen
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
- Automatische Zugangssperre und Manuelle Zugangssperre

1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen werden, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Erstellen eines Berechtigungskonzepts
- Umsetzung von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen

1.4 Verwendungszweckkontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Datensparsamkeit im Umgang mit personenbezogenen Daten
- Getrennte Verarbeitung verschiedener Datensätze
- Regelmäßige Verwendungszweckkontrolle und Löschung
- Trennung von Live-/Test- und Entwicklungsumgebung

1.5 Datenschutzfreundliche Voreinstellungen

Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
- Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
- Protokollierung von Übermittlungen gemäß Protokollierungskonzept
- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Sichere Übertragung zu externen Systemen
- Risikominimierung durch Netzseparierung
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Härtung der Backendsysteme
- Beschreibung der Schnittstellen

- Umsetzung einer Maschine-Maschine-Authentisierung
- Sichere Ablage von Daten, inkl. Backups
- Gesicherte Speicherung auf mobilen Datenträgern
- Einführung eines Prozesses zur Datenträgerverwaltung
- Prozess zur Sammlung und Entsorgung
- Datenschutzgerechter Lösch- und Zerstörungsverfahren
- Führung von Löschprotokollen

2.2 Eingabekontrolle

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingaben
- Dokumentation der Eingabeberechtigungen

3. Verfügbarkeit, Belastbarkeit, Disaster Recovery

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

- Brandschutz
- Redundanz der Primärtechnik
- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Monitoring
- Ressourcenplanung und Bereitstellung
- Abwehr von systembelastendem Missbrauch
- Datensicherungskonzepte und Umsetzung
- Regelmäßige Prüfung der Notfalleinrichtungen

3.2 Disaster Recovery – rasche Wiederherstellung nach Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

- Notfallplan
- Datensicherungskonzepte und Umsetzung

4. Datenschutzorganisation

- Festlegung von Verantwortlichkeiten
- Umsetzung und Kontrolle geeigneter Prozesse
- Melde- und Freigabeprozess

- Umsetzung von Schulungsmaßnahmen
- Verpflichtung auf Vertraulichkeit
- Regelungen zur internen Aufgabenverteilung
- Einführung einer geeigneten Vertreterregelung

5. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl weiterer Auftragnehmer nach geeigneten Garantien
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Informationssicherheitsmanagement
- Prozess zur Evaluation der technischen und organisatorischen Maßnahmen
- Prozess Sicherheitsvorfall-Management
- Durchführung von technischen Überprüfungen

Linz _____, den 04.11.2025
Ort Datum

04.11.2025 09:04:20
Digital unterzeichnet auf
my.world4you.com mit Login 50312781

- Auftraggeber -



- Auftragnehmer -