**Vertrag über die Auftragsverarbeitung**

**personenbezogener Daten**

|  |  |
| --- | --- |
| zwischen | und |
| Name des KundenStraße und NummerPostleitzahl und Ort | **EurOwiG AG** Am Unteren Stein 486672 Thierhaupten |
| vertreten durch | vertreten durch |
| Name der vertretenden Person | **Frau Gabriela Wagner** |
| Im Folgenden **Auftraggeber** | Im Folgenden **Auftragnehmer** |

[1. Einleitung, Geltungsbereich, Definitionen 1](#_Toc136442259)

[2. Gegenstand und Dauer der Verarbeitung 1](#_Toc136442260)

[3. Pflichten des Auftragnehmers 2](#_Toc136442261)

[4. Technische und organisatorische Maßnahmen 3](#_Toc136442262)

[5. Regelungen zur Berechtigung, Löschung und Sperrung von Daten 4](#_Toc136442263)

[6. Unterauftragsverhältnisse 4](#_Toc136442264)

[7. Rechte und Pflichten des Auftraggebers 5](#_Toc136442265)

[8. Mitteilungspflichten 6](#_Toc136442266)

[9. Weisungen 6](#_Toc136442267)

[10. Beendigung des Auftrags 7](#_Toc136442268)

[11. Vergütung 7](#_Toc136442269)

[12. Sonderkündigungsrecht 7](#_Toc136442270)

[13. Haftung 8](#_Toc136442271)

[14. Sonstiges 8](#_Toc136442272)

[Anlage 1 – Technische und organisatorische Maßnahmen 9](#_Toc136442273)

[Anlage 2 – Zugelassene Subdienstleister 11](#_Toc136442274)

[Anlage 3 – Weisungsberechtigte Personen 12](#_Toc136442275)

# 1. Einleitung, Geltungsbereich, Definitionen

1. Dieser Vertrag regelt die Rechte und Pflichten von Aufraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutz-Grundverordnung zu verstehen. 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 Gegenstand des Auftrags (die Dienstleistung des Auftragnehmers) besteht in der Fernwartung und Serviceleistung (z.B. Datenanalyse, Datenkorrektur) in allen EurOwiG Fachverfahren, inklusive aller Module, Auswertungstools und Schnittstellen. Nachträgliche Änderungen sind schriftlich zu vereinbaren.

## 2.2 Dauer

Die Verarbeitung erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrages oder des „Vertrages über die Pflege von Standardsoftware“ (Hauptvertrag) durch eine Partei. Der Auftrag kann von beiden Parteien mit einer Frist von 3 Monaten zum Quartalsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

## 2.3 Art und Zweck der Verarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im abgeschlossenen Hauptvertrag.

Die Verarbeitung ist folgender Art:

Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

Der zugrundeliegende Zweck der Verarbeitung ist in der Leistungsbeschreibung des Hauptvertrages geregelt.

## 2.4 Art der Daten

Es werden folgende Daten verarbeitet:

* Personenstammdaten
* Kommunikationsdaten (z. B. Telefon, E-Mail)
* Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
* Kundenhistorie
* Vertragsabrechnungs- und Zahlungsdaten
* Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

## 2.5 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

* Kunden / Betroffene
* Beschäftigte
* Ansprechpartner

# 3. 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 hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle 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.

Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Frau Gabriela Wagner, Geschäftsleitung, datenschutz@eurowig.de benannt.

1. Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR.

Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

# 4. Technische und organisatorische Maßnahmen

1. Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.
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 Daten-beständen strikt getrennt werden.
5. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
6. Die Verarbeitung von Daten in Privatwohnungen ist gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird. Sämtliche Mitarbeiter sind zur Vertraulichkeit verpflichtet und werden regelmäßig im Bereich Datenschutz sensibilisiert. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.
7. Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

# 5. Regelungen zur Berechtigung, Löschung und Sperrung von Daten

1. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
2. Entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

# 6. Unterauftragsverhältnisse

1. Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunter-nehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.
2. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzu-ziehung oder Ersetzung des Subunternehmers informiert der Auftragnehmer den Auftraggeber.

Der Auftraggeber hat das Recht innerhalb von zwei Wochen ab Kenntnis der Information über den Subdienstleister aus wichtigem Grund schriftlich beim Auftragnehmer Einspruch gegen den Einsatz des Subunternehmers einzulegen. Erfolgt kein Einspruch innerhalb der genannten Frist, gilt dies als Zustimmung des Auftraggebers zum Einsatz dieses Subdienstleisters.

1. Subunternehmern sind vertraglich mindestens die Datenschutzverpflichtungen auferlegt, die in den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
2. Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
3. Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig von-einander abzugrenzen.
4. Eine weitere Subbeauftragung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers (mindestens Textform); sämtliche vertragliche Regelungen zu den Datenschutzpflichten in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.
5. Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
6. Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.
7. Es werden nur Subunternehmen innerhalb der EU oder des EWR beauftragt.
8. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.
9. Kommt der Subunternehmer seinen Datenschutzverpflichtungen nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

# 7. 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.

(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. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 4 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

# 8. Mitteilungspflichten

1. Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle sind mitzuteilen. Die Mitteilung hat mindestens die Angaben nach Art. 33 Abs. 3 Datenschutz-Grundverordnung zu enthalten.
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.

# 9. 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.

# 10. Beendigung des Auftrags

1. Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben und sodann zu vernichten. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Gleiches gilt für Test- und Ausschussmaterial.
2. Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
3. Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
4. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

# 11. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

# 12. 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 ist zur außerordentlichen Kündigung berechtigt, sofern der Auftraggeber der Beauftragung eines Subunternehmers gem. Kapitel 6 (1) dieses Vertrages widerspricht und keine Einigung erreicht werden kann.

# 13. Haftung

1. Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Daten-verarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftrag-nehmer als Gesamtschuldner.
2. Soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist, stellt der Auftraggeber den Auftragnehmer auf erste Anforderung von sämtlichen Ansprüchen Dritter frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftragnehmer erhoben werden.
3. Der Auftragnehmer haftet dem Auftraggeber gegenüber nur bei grober Fahrlässigkeit oder Vorsatz.

# 14. 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 erforderlich.
4. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
5. Der Gerichtsstand für beide Parteien ist der Sitz des Auftragnehmers.
6. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

**Unterschriften**

Ort, Datum Ort, Datum

Ort, Datum Thierhaupten, Datum

Unterschrift Auftraggeber

Auftraggeber EurOwiG AG

**Hinweis**: Es handelt sich bei dieser Vereinbarung um einen echten Vertrag, der dementsprechend von einer für das Unternehmen vertretungsbefugten Person zu zeichnen ist. Der DSB ist dies in aller Regel nicht.

# Anlage 1 – Technische und organisatorische Maßnahmen

Im Folgenden werden die 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.

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

*Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.*

Zutrittskontrollsystem, Schlüssel / Schlüsselvergabe, Türsicherung mit biometrischer Zugangskontrolle (Fingerprint), Alarmanlage.

1. **Zugangskontrolle**

*Eine unbefugte Systemnutzung ist zu verhindern.*

Sichere Kennwörter, automatische PC-Sperrmechanismen, Verschlüsselung von Datenträgern, Einrichtung eines Benutzerstammsatzes pro Mitarbeiter.

Der externe Zugriff auf das Firmennetz für Mitarbeiter im Außeneinsatz ist durch ein VPN abgesichert.

1. **Zugriffskontrolle / Benutzerkontrolle**

*Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems möglich sein.*

Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte durch Microsoft Active Directory, Protokollierung von Zugriffen.

Weiter sind alle Clientrechner auf Datenträgerebene verschlüsselt, so dass der unbefugte Zugriff auf die gespeicherten Daten nicht möglich ist.

1. **Trennungskontrolle**

*Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden.*

Mandantenfähigkeit / Zweckbindung, Sandboxing, Funktionstrennung / Produktion / Test

1. **Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DS-GVO, Art. 25 Abs. 1 EU-DS-GVO)**

*Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.*

Die EurOwiG Produkte stellen entpersonalisierte LOG-Files zur Verfügung. Die Annahme von nicht-entpersonalisierten Datensätzen wird verweigert und gegebenenfalls übermittelte Daten werden unwiderruflich gelöscht.

1. **Integrität (Art. 32 Abs. 1 lit. b EU-DS-GVO)**
2. **Weitergabekontrolle / Übertragungskontrolle**

*Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.*

Verschlüsselung, Virtual Private Networks (VPN), Transportsicherung

1. **Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle**

*Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

Protokollierung, Dokumentenmanagement, passwortgeschützt

**3. Verfügbarkeit und Belastbarkeit / Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b EU-DS-GVO)**

*Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.*

Backup-Strategie (online / offline; on-site / off-site), unterbrechungsfreie Stromversorgung (USV), Spiegeln von Festplatten - RAID-Verfahren, Getrennte Aufbewahrung, Virenschutz, Firewall, Meldewege und Notfallpläne; darüber hinaus: rasche Wiederherstellbarkeit, Art. 32 Abs. 1 lit. c EU-DS-GVO

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

1. **Datenschutz-Management**
2. **Incident-Response-Management**
3. **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DS-GVO)**
4. **Auftragskontrolle**

*Keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers*

Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen

# Anlage 2 – Zugelassene Subdienstleister

Für Anwender, die ein EurOwiG Online Produkt (Mobile Smart, Anhörung Online, WebApp) einsetzen, und bei der EurOwiG AG die Daten und Anwendungen hosten, kommen folgende Unterauftragsverarbeiter zum Einsatz:

|  |  |
| --- | --- |
| **Unterauftragsverarbeiter** | **Durchzuführende Tätigkeit(en)** |
| **NCS Netzwerke Computer Service GmbH**Balthasar-Schaller-Str. 886316 Friedberg**Vertreten durch:**Stefan Schneider / Joachim Böttcher | • Hosting• Bereitstellung von Serverhardware und Software• Datensicherung• Zugriffsschutz |

Für alle Anwender, die ein EurOwiG Produkt einsetzen, kommen folgende Unterauftragsverarbeiter zum Einsatz:

|  |  |
| --- | --- |
| **Unterauftragsverarbeiter** | **Durchzuführende Tätigkeit(en)** |
| **DATEV eG, Nürnberg**Paumgartnerstr. 6 – 1490429 Nürnberg**Vorsitzender des Aufsichtsrates:**Nicolas Hofmann | * Buchhaltung
 |
| **NCS Netzwerke Computer Service GmbH**Balthasar-Schaller-Str. 886316 Friedberg**Vertreten durch:**Stefan Schneider / Joachim Böttcher | * Speicherung von allgemeinen Kundendaten und Kontaktdaten
 |
| **Microsoft Deutschland GmbH**Walter-Gropius-Straße 580807 München**Vertreten durch:**Dr. Marianne Janik  | * Kommunikation Outlook E-Mail
 |
| **Mailjet GmbH**Alt-Moabit 210557 Berlin**Vertreten durch**:Tim Keithahn / Will Conway | * Versand von Updatebenachrichtigungen
 |
| **netcup GmbH**Daimlerstraße 2576185 Karlsruhe**Vertreten durch:**Oliver Werner / Alexander Windbichler | * Betrieb der Cloudlösung: Bereitstellung von Updates und Produktinformationen
 |

Die Zustimmung zum Einsatz des/der oben genannten Unterauftragsverarbeiters/ Unterauftragsverarbeiter für die genannten durchzuführenden Tätigkeiten wird erteilt, sofern die datenschutzrechtlichen Voraussetzungen entsprechend dieser Vereinbarung auch in diesem Vertrags-verhältnis (Unterauftragsverarbeiter-ADV) eingehalten werden.

# Anlage 3 – Weisungsberechtigte Personen

**Weisungsberechtigte Personen des Auftraggebers sind:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Weisungsberechtigte Person ist stets die Person im oben genannten Amt. Bei einem Wechsel der Person liegt die Weisungsberechtigung bei dem neuen Amtsinhaber.*

**Weisungsempfänger beim Auftragnehmer sind:**

Mitarbeiter der Firma EurOwiG AG, die das Fachverfahren EurOwiG inklusive aller Module, Auswertungstools und Schnittstellen betreuen.

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

Weisungen des Auftraggebers an den Auftragnehmer werden ausschließlich von den o. g. verantwortlichen Sachgebietsbearbeitern erteilt.