

# Vereinbarung zur Auftragsbearbeitung

zwischen

_____	Firma
_____	Name
_____	Strasse, Nr.
_____	PLZ, Ort

**Verantwortliche – nachfolgend «Kundin» genannt**

und

rockIT AG  
Albulastrasse 47  
8048 Zürich

**Auftragsbearbeiterin - nachfolgend «Anbieterin» genannt**

(Kundin und Anbieterin je einzeln eine "Partei" und zusammen die "Parteien")

## A. Allgemeine Bestimmungen

### 1. Gegenstand und Anwendungsbereich dieser Vereinbarung

- 1.1 Diese Vereinbarung über die Auftragsbearbeitung ("**Vereinbarung**") konkretisiert die Rechte und Pflichten der Parteien in Bezug auf die Auftragsbearbeitung, die sich für sie aus dem anwendbaren Datenschutzrecht ergeben. Sie ergänzt diesbezüglich die vertraglichen Vereinbarungen zwischen den Parteien. Dabei kann es sich um einen einzelnen oder mehrere Verträge zwischen den Parteien über die Leistungserbringung für die Kundin handeln ("**Vertrag**").
- 1.2 Die Vereinbarung gilt nur in Bezug auf Dienstleistungen, bei denen die Anbieterin Personendaten im Auftrag und für Zwecke der Kundin bearbeitet ("**Auftragsbearbeitung**"), wobei die Kundin entweder Verantwortliche oder Auftragsbearbeiterin und die Anbieterin entweder Auftragsbearbeiterin oder Unter-Auftragsbearbeiterin ist.
- 1.3 Diese Vereinbarung wird mit ihrer gegenseitigen Unterzeichnung durch die Parteien verbindlich.

1.4 Diese Vereinbarung ist ein integraler Bestandteil des Vertrags. Die Bestimmungen dieser Vereinbarung schränken die Rechte und Pflichten der Parteien in Bezug auf die Erbringung von Dienstleistungen unter dem Vertrag nicht ein. Ihren Regelungsgegenstand betreffend gehen die Bestimmungen dieser Vereinbarung indes den Bestimmungen des Vertrags vor.

## **2. Laufzeit der Vereinbarung**

2.1 Die Laufzeit dieser Vereinbarung entspricht der Dauer des Vertrags, sofern sich aus den Bestimmungen dieser Vereinbarung keine zeitlich darüberhinausgehenden Verpflichtungen ergeben. Bei solchen überdauernden Verpflichtungen besteht diese Vereinbarung so lange fort, bis die entsprechenden Verpflichtungen erloschen sind.

2.2 Durch diese Regelung modifizieren die Parteien nicht die im Vertrag vereinbarten Kündigungsrechte.

## **3. Definitionen**

3.1 Die in dieser Vereinbarung in Fettschrift hervorgehobenen und in Anführungs- und Schlusszeichen gesetzten Begriffe haben in der gesamten Vereinbarung die ihnen darin zugeschriebene Bedeutung.

3.2 Die in dieser Vereinbarung verwendeten datenschutzbezogenen Begriffe wie "Personendaten" (personenbezogene Daten), "betroffene Person", "Verantwortlicher", "Auftragsbearbeiter", oder "Datenschutz-Folgenabschätzung" haben die ihnen im Schweizer DSG bzw. (wo anwendbar) in der EU-DSGVO zugeschriebene Bedeutung.

## **B. Beschreibung der Auftragsbearbeitung und Pflichten der Parteien**

### **4. Angaben zur Auftragsbearbeitung und Zweck**

4.1 Gegenstand und Zweck der Auftragsbearbeitung ergeben sich aus dem Vertrag und den Leistungsbeschreibungen der Anbieterin in Verbindung mit allfälligen separaten Weisungen der Kundin.

4.2 Die Art der Bearbeitung, die Art der bearbeiteten Personendaten ("vertragsgegenständliche Personendaten") und der Kreis (Kategorien) betroffener Personen bestimmen sich ebenfalls nach dem Vertrag und den Leistungsbeschreibungen der Anbieterin in Verbindung mit allfälligen separaten Weisungen der Kundin.

4.3 Die Auftragsbearbeitung erfolgt in der Schweiz.

4.4 Die Dauer der Bearbeitung bestimmt sich nach Ziffer 2.

### **5. Weisungsgebundenheit, Zweckbindung und Kontrolle**

Die Anbieterin verpflichtet sich und sichert zu, dass die Anbieterin alle vertragsgegenständlichen Personendaten (i) ausschliesslich zu den in Ziffer 4 beschriebenen Zwecken, (ii) in Übereinstimmung mit den Weisungen der Kundin sowie (iii) in Übereinstimmung mit dieser Vereinbarung bearbeitet; und (iv) nicht für eigene Zwecke verwendet.

### **6. Datensicherheit**

6.1 Die Anbieterin verpflichtet sich, im Interesse der Vertraulichkeit, Integrität und vertragsgemässen Verfügbarkeit der vertragsgegenständlichen Personendaten angemessene technische und organisatorische Schutzmassnahmen zu treffen.

6.2 Die Anbieterin implementiert hierzu insbesondere Zugangskontrollen, Zugriffskontrollen sowie Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen. Bei der Auswahl der Massnahmen berücksichtigt die Anbieterin den Stand der Technik, die Implementierungskosten sowie die Art, den Umfang, die Umstände und die Zwecke der Bearbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für betroffene Personen.

## 7. Meldung von Verletzungen der Datensicherheit

7.1 Wenn die Anbieterin eine Verletzung der Sicherheit bemerkt, die darin besteht, dass vertragsgegenständliche Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden ("**Verletzung der Datensicherheit**"), wird die Anbieterin die Verletzung der Datensicherheit so rasch als möglich und ohne schuldhaftes Zögern der Kundin melden. Die Anbieterin wird die Verletzung der Datensicherheit sodann (i) untersuchen und die Auswirkungen ermitteln, (ii) die Kundin detailliert über die Verletzung der Datensicherheit informieren und (iii) angemessene Massnahmen ergreifen, um die Auswirkungen zu mildern und das Risiko, das sich aus der Verletzung der Datensicherheit für betroffene Personen möglicherweise ergibt, so gering wie möglich zu halten.

7.2 Die Anbieterin wird die Kundin in angemessener Weise unterstützen, um die Kundin bei der Erfüllung ihrer Verpflichtungen zu unterstützen, Verletzungen der Datensicherheit an zuständige Aufsichtsbehörden oder an betroffene Personen zu melden.

## 8. Informations- und Unterstützungspflichten

8.1 Die Anbieterin verpflichtet sich, die Kundin so rasch als möglich und von sich aus zu informieren, (i) wenn die Anbieterin der Ansicht ist, dass die Anbieterin in absehbarer Zeit nicht mehr in der Lage ist, den Pflichten gemäss dieser Vereinbarung nachzukommen; sowie (ii) über jede Anfrage zur Ausübung von Betroffenenrechten, welche die Anbieterin direkt von betroffenen Personen in Bezug auf vertragsgegenständliche Personendaten erhalten hat (vorausgesetzt, die Anbieterin kann eine Zuordnung an die betroffene Person gestützt auf die Angaben der betroffenen Person vornehmen; andernfalls wird die Anbieterin die betroffene Person bitten, sich an die für die Datenbearbeitung Verantwortliche zu wenden).

8.2 Die Anbieterin verpflichtet sich, die Kundin auf Anfrage und gegen separate Vergütung bei der Beantwortung von Anfragen betroffener Personen zur Ausübung datenschutzrechtlicher Betroffenenrechte zu unterstützen.

8.3 Zudem verpflichtet sich die Anbieterin, die Kundin auf Anfrage und gegen separate Vergütung bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen von Datenschutzaufsichtsbehörden zu unterstützen.

8.4 Die Anbieterin stellt der Kundin alle Informationen zur Verfügung, welche die Kundin vernünftigerweise für den Nachweis der Einhaltung ihrer Verpflichtungen aus dem anwendbaren Datenschutzrecht in Bezug auf die Auftragsbearbeitung benötigt. Auf Anfrage der Kundin stellt die Anbieterin zudem allfällige Berichte zur Informationssicherheit bereit, die eine Prüfgesellschaft oder Zertifizierungsstelle in Bezug auf die Dienstleistungen der Anbieterin oder ihrer Unter-Auftragsbearbeiter erstellt hat.

## 9. Geheimhaltung

9.1 Die Anbieterin verpflichtet sich zur Geheimhaltung der vertragsgegenständlichen Personendaten und hat die mit der Auftragsbearbeitung betrauten Personen zur Wahrung der Vertraulichkeit zu verpflichten.

9.2 Diese Geheimhaltungsverpflichtungen gelten auch nach Beendigung dieser Vereinbarung für unbeschränkte Dauer weiter.

## **10. Unter-Auftragsbearbeiter**

10.1 Unter-Auftragsbearbeiter sind natürliche oder juristische Personen, welche die Anbieterin für die Auftragsbearbeitung beizieht. Die Anbieterin ist berechtigt, Unter-Auftragsbearbeiter beizuziehen. Die Anbieterin ist in solchen Fällen verpflichtet, mit Unter-Auftragsbearbeitern im erforderlichen Umfang eine Vereinbarung über die (Unter-)Auftragsbearbeitung zu treffen, die der Anbieterin die Einhaltung der Bestimmungen der vorliegenden Vereinbarung zwischen der Anbieterin und der Kundin ermöglicht. Dies beinhaltet auch die Überbindung der Geheimhaltungspflichten der Anbieterin auf den Unter-Auftragsbearbeiter.

10.2 Die Anbieterin wird die Kundin sechs (6) Monate vorab in geeigneter Weise schriftlich informieren, wenn die Anbieterin nach Inkrafttreten dieser Vereinbarung beabsichtigt, neue Unter-Auftragsbearbeiter beizuziehen oder bestehende auszutauschen. Wenn die Kundin dem Bezug bzw. Austausch des Unter-Auftragsbearbeiters nicht innerhalb von dreissig (30) Tagen nach dem Datum der Mitteilung schriftlich widerspricht, gilt der neue oder ausgetauschte Unter-Auftragsbearbeiter als genehmigt.

10.3 Die Kundin hat einen allfälligen Widerspruch gegen den neuen oder ausgetauschten Unter-Auftragsbearbeiter zu begründen. Erfolgt der Widerspruch aus zwingenden gesetzlichen oder regulatorischen Gründen, so kann die Anbieterin wahlweise einen anderen Unter-Auftragsbearbeiter beiziehen oder der Kundin ein ausserordentliches Kündigungsrecht gewähren. Erfolgt der Widerspruch nicht aus gesetzlich oder regulatorisch zwingenden Gründen und hält die Anbieterin am Unter-Auftragsbearbeiter fest, so initiiert die Anbieterin einen Einigungsversuch mit der Kundin, zu dem die Anbieterin weitere Parteien (namentlich andere Kundinnen der Anbieterin und den Unter-Auftragsbearbeiter) beiziehen kann. Scheitert der Einigungsversuch, steht es der Kundin frei, auf die Nutzung der Dienstleistungen zu verzichten und den Vertrag ausserordentlich zu kündigen.

## **11. Rückgabe oder Löschung vertragsgegenständlicher Personendaten bei Vertragsbeendigung**

Die Anbieterin wird die vertragsgegenständlichen Personendaten nach Beendigung des Vertrags nach Massgabe der diesbezüglichen Bestimmungen im Vertrag löschen oder, wenn diese dies wünscht, in einem geeigneten Format an die Kundin zurückgeben.

## **12. Audit**

12.1 Die Kundin kann bei der Anbieterin einmal jährlich ein Audit zur Prüfung der Sicherheitsmassnahmen oder der sonstigen Einhaltung dieser Vereinbarung durchführen oder durchführen lassen. Die Kosten dafür trägt die Kundin. Die Anbieterin unterstützt die Audits im Rahmen eines verhältnismässigen Aufwands unentgeltlich.

12.2 Die Prüfungs- und Auditrechte gemäss dieser Vereinbarung gelten nur insoweit als der Vertrag der Kundin nicht anderweitig erlaubt, die Erfüllung dieser Vereinbarung durch die Anbieterin zu prüfen und zu auditieren.

Für \_\_\_\_\_ (Kundin):

Unterschrift: ..... Unterschrift: .....

Name: ..... Name: .....

Datum: ..... Datum: .....

Für rockIT AG:

Unterschrift: ..... Unterschrift: .....

Name: ..... Name: .....

Datum: ..... Datum: .....