Auftragsdatenbearbeitungsvertrag

Dieser Auftragsdatenbearbeitungsvertrag (gem. Art. 9 DSG) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner, welche sich aus dem bestehenden Vertragsverhältnis und den jeweils erteilten Einzelaufträgen und den darin enthaltenen Pflichten zwischen der Comatic AG (nachfolgend «Auftragnehmer») und ihren Kundinnen und Kunden (nachfolgend «Auftraggeber») ergeben. Dieser findet Anwendung auf alle Datenbearbeitungen, die der Auftragsnehmer im Auftrag des Auftragsgeber vornimmt.

In diesem Vertrag werden Gegenstand und Dauer der Bearbeitung, Art und Zweck der Bearbeitung, die Art der Personendaten, die Kategorien betroffener Personen und die Pflichten und Rechte der Vertragspartner beschrieben.

1. Gegenstand und Dauer der Auftragsdatenbearbeitung

1.1. Der Auftragnehmer bearbeitet Personendaten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die durch das bestehenden Vertragsverhältnis sowie durch die erteilten Einzelaufträge konkretisiert werden.

1.2. Ergänzend hierzu gilt je nach Einzelauftrag folgende Beschreibungen des Gegenstands der Bearbeitung:

- Hosting und / oder der Bereitstellung von Softwareanwendungen in einem Rechenzentrum
- Supportleistungen im Rahmen der Nutzung der Softwareanwendung (Bsp. Fernwartung, Datensicherung etc.)
- Betrieb, Support und Wartungsarbeiten an der ICT-Infrastruktur
- Sonstige IT-Dienstleistungen

1.3. Die Laufzeit der Vereinbarung richtet sich nach der Laufzeit des bestehenden Vertragsverhältnisses und der erteilten Einzelaufträge und tritt mit der Nutzung der Software oder dem Erteilen eines Einzelauftrages in Kraft.

1.4. Es findet grundsätzlich eine Bearbeitung von Personendaten von Personen, welche in der Schweiz wohnhaft sind, statt. Sollte eine Bearbeitung von Personen, wohnhaft in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Auftragsdatenbearbeitungsvertrag stattfinden, sind die nach DSG verwendeten Begriffe, soweit anwendbar, auch im Sinne der DSGVO zu verstehen.

2. Art und Zweck der Bearbeitung

2.1. Über Art und Zweck der Bearbeitung entscheidet der Auftraggeber.

2.2. Insbesondere können folgende Personendaten durch den Auftragnehmer im Auftrag des Auftraggebers bearbeitet werden:

- Personenstammdaten (Name, Geburtsdatum, Anschrift, Arbeitgeber, Sozialversicherungsdaten) einschliesslich Kontaktdaten (Bsp. Telefon, E-Mail)
- Lohn- und Finanzdaten, Zeitdaten, Krankheits- und Unfalldaten
- Vertragsdaten, einschliesslich Abrechnung und Zahlungsdaten, geschäftliche Korrespondenz
- Benutzer- und Logindaten

- Historie der Vertragsdaten
- Details aus Geschäftsbeziehungen

3. Kategorien betroffener Personen

3.1. Die Kategorien der betroffenen Personen hängen von den durch den Auftraggeber übermittelte Daten ab. Diese sind insbesondere (abhängig vom Auftrag):

- Mitarbeiter (einschliesslich Bewerber und ehemaligen Mitarbeitern) des Auftraggebers
- Kunden des Auftraggebers
- Interessenten des Auftraggebers
- Dienstleister und Lieferanten des Auftraggebers
- Partner des Auftraggebers
- Kontaktdaten zu Ansprechpartnern

4. Weisungsgebundenheit

4.1. Der Auftragnehmer darf Daten nur im Rahmen des Auftrages, d.h. im Rahmen der sich aus dem bestehenden Vertragsverhältnis und den erteilten Einzelaufträgen ergebenden Bestimmungen und Weisungen des Auftraggebers verarbeiten.

4.2. Der Auftraggeber ist als Verantwortlicher im Sinne von Art. 5 lit. j DSG im Rahmen dieses Vertrags für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmässigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmässigkeit der Datenbearbeitung verantwortlich. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit und nach Beendigung dieses Vertrags Weisungen an den Auftragnehmer ersteilen.

4.3. Jede Weisung des Auftraggebers bedarf der Schrift- oder Textform (Bsp. Brief, E-Mail) und muss nachvollziehbar dokumentiert werden. Es muss stets nachvollzogen werden können, wann und von wem eine Weisung an den Auftragnehmer erteilt wurde. Der Auftragnehmer hat nur Weisungen in Schrift- oder Textform zu befolgen.

4.4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen das DSG oder gegen andere Datenschutzbestimmungen der Schweiz verstösst.

5. Vertraulichkeit

5.1. Der Auftragnehmer gewährleistet und versichert, dass sich die zur Bearbeitung der Personendaten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.2. Der Auftragnehmer erbringt auf Anfrage den Nachweis über die Verpflichtung auf Vertraulichkeit.

6. Technische und organisatorische Massnahmen (TOM)

6.1. Unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Bearbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher

Personen hat der Auftragsnehmer geeignete technische und organisatorische Massnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Massnahmen schliessen unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung der Personendaten
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Bearbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der Personendaten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung.

6.2. Bei der Beurteilung der eingesetzten TOM hat der Auftragnehmer die Risiken für die Persönlichkeitsrechte der Betroffenen bei einer allfälligen Verletzung der Datensicherheit berücksichtigt.

6.3. Zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten hat der Auftragsnehmer die in seinem Datenschutz- und Datensicherheitskonzept aufgeführten technischen und organisatorischen Massnahmen getroffen. Die Beschreibung der technischen und organisatorischen Massnahmen nach Art. 7, 8 DSG ist im Anhang A aufgeführt.

7. Subunternehmer (weitere Auftragsbearbeitern)

7.1. Der Auftragnehmer nimmt keinen weiteren Auftragsbearbeiter ohne vorherige gesonderte schriftliche Genehmigung des Auftraggebers in Anspruch.

7.2. Erteilt der Auftragsnehmer nach vorgängiger Genehmigung Aufträge an weitere Auftragsbearbeiter, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem weiteren Auftragsbearbeiter zu übertragen.

7.3. Für den Fall, dass der Auftraggeber ein Cloud-Produkt (siehe Anhang C, Übersicht der Cloud-Produkte mit jeweiligen Hoster) beim Auftragnehmer bestellt, erteilt der Auftraggeber bereits hiermit seine ausdrückliche vorgängige Genehmigung dazu, dass der Auftragnehmer zur Begründung eines Unterauftragsverhältnisses nach Massgabe der hier vereinbarten Regelungen mit dem entsprechenden Hoster berechtigt ist.

8. Rechte der Betroffenen

8.1. Falls das Begehren an den Auftragnehmer gestellt wird, informiert der Auftragnehmer den Auftraggeber über dieses Begehren. Die Verantwortung der Auskunftserteilung verbleibt beim Auftragsgeber. Der Auftragnehmer unterstützt den Auftraggeber auf Anfrage mit verhältnismässigem Aufwand.

8.2. Der Auftragnehmer trifft insbesondere geeignete technische und organisatorische Massnahmen, um dem Auftraggeber die Erfüllung seiner Pflichten gegenüber den Betroffenen zu ermöglichen.

9. Unterstützungspflicht

9.1. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Bearbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 8, Art. 24 sowie

Art. 25 DSG genannten Pflichten zur Sicherheit der Bearbeitung von Personendaten sowie zu etwa bestehenden Melde- und Benachrichtigungspflichten.

9.2. Der Auftragnehmer stellt ein angemessenes Schutzniveau durch technische und organisatorische Massnahmen sicher, welche die Umstände und Zwecke der Bearbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

9.3. Der Auftragnehmer ist verpflichtet, eine Verletzung des Schutzes der Personendaten unverzüglich an den Auftraggeber zu melden. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Meldeverpflichtung aus Art 24 DSG und stellt ihm die benötigten Informationen unverzüglich zur Verfügung.

10. Beendigung der Erbringung der Bearbeitungsleistungen

10.1. Nach Beendigung des bestehenden Vertragsverhältnisses und des jeweiligen Einzelauftrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlangen, Daten und erstellten Bearbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

10.2. Die Daten auf den Datenträger des Auftragnehmers sind, vorbehältlich allfälliger gesetzlicher Aufbewahrungspflichten, nach Beendigung des bestehenden Vertragsverhältnisses und des jeweiligen Einzelauftrages physisch zu löschen. Die Löschung ist – auf Verlangen des Auftraggebers – in geeigneter Weise zu dokumentieren.

11. Nachweispflicht

11.1. Der Auftraggeber hat das Recht, sich vor der Aufnahme der Datenbearbeitung und sodann regelmässig von den technischen und organisatorischen Massnahmen des Auftragsnehmer zu überzeugen. Hierfür kann er insbesondere Selbstauskünfte des Auftragnehmers einholen und sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufes persönlich überzeugen oder einen Dritten hiermit beauftragen. Die dafür anfallenden Kosten können dem Auftraggeber übertragen werden.

11.2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

12. Berechtigung, Einschränkung und Löschung von Daten

12.1. Der Auftragnehmer darf die Daten ausschliesslich gem. Einzelvertrag oder auf schriftliche Weisung des Auftraggebers bearbeiten.

13. Dokumentationspflicht

13.1. Der Auftragnehmer führt ein Verzeichnis der Bearbeitungstätigkeiten (Art, 12 Abs.3) welches Folgendes enthält:

a) die Identität des Verantwortlichen und des Auftragsbearbeiters sowie eines etwaigen Datenschutzberaters;
b) die Kategorien von Bearbeitungen, die im Auftrag jedes Auftraggebers durchgeführt werden;

c) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Massnahme gem. Art. 8 DSG.

13.2. Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

14. Schlussbestimmungen

14.1. Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschliesslich etwaiger Zusicherungen des Auftragnehmers – bedürften einer schriftlichen Vereinbarung, mindestens in Textform, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

14.2. Es gilt Schweizer Recht. Gerichtsstand ist der Sitz des Auftraggebers.

14.3. Sollten einzelne Teile des Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Bestimmungen des Auftragsbearbeitungsvertrag nicht.

Für sämtliche anfallenden Fragen zum Datenschutz und dem Auftragsdatenbearbeitungsvertrag steht dem Auftraggeber die zentrale Stelle für den Datenschutz der Comatic AG unter datenschutz@comatic.ch zur Verfügung.

Anhang A, Anhang B und Anhang C sind wesentliche Bestandteile des Auftragsdatenbearbeitungsvertrags.

Stand: August 2023

Comatic AG
Rathausplatz 9
6210 Sursee

Anhang A	Beschreibung der technischen und organisatorischen Massnahmen (TOM)
Anhang B	Verzeichnis der Unterauftragsbearbeiter mit vorgängiger Genehmigung
Anhang C	Übersicht der Cloud-Produkte mit jeweiligem Hoster

Comatic

Comatic AG
Rathausplatz 9
6210 Sursee

Anhang A – Beschreibung der technischen und organisatorischen Massnahmen (TOM)

Kontrollziele	Massnahmen
Pseudonymisierung und Verschlüsselung personenbezogener Daten	• HTTPS-Verschlüsselung in der Webkommunikation • RDP-Verschlüsselung der Remotedesktopkommunikation • Verschlüsselung aller Datensicherungen
Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste in Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	• Zugangsschutz (Authentisierung) • Einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau • Zentraler, verschlüsselter Password-Safe für alle Beschäftigte • Sperrung bei Fehlversuchen und Prozess zur Rücksetzung gesperrter Zugangserkennung • Berechtigte können nur auf für sie berechtigte Daten zugreifen • Einsatz eines Firewall- und Proxy-Systems • Verpflichtung der Mitarbeiter auf das Datengeheimnis • Schutz vor Viren- und Spionagesoftware auf allen Server und Arbeitsplätze • Redundante Hardware für die Serverinfrastruktur • Regelmässige Prüfung und Backup der Hardwarekonfigurationen • Redundante Internetanbindung • Klimaanlagen und USV in Serverräumen • Festlegung der berechtigten Personen für den Zugang zum Rechenzentrum • Besucher des Rechenzentrums (Bsp. für Wartungszwecke) werden zwingend begleitet • Sichere Löschung von Datenträger • Regelungen zur Kontrolle von externer Wartung und Fernwartung • Brandmeldeanlage
Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	• Doppelt- oder Mehrfachvorhaltung aller Komponenten in der Datenverarbeitung • Datensicherungs- und Wiederherstellungskonzept • Dezentrale Backuplösung • Unterbrechungsfreie Stromversorgung • Überwachungs- und Meldesysteme
Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Verarbeitung	• Regelmässige Prüfung, ob/in welchem Umfang Zugangsrechte noch erforderlich sind • Regelmässige Prüfung, ob/in welchem Umfang Zugriffsrechte noch erforderlich sind • Incident-Response Management • Auftragskontrolle bei Auftragsverarbeitung
Trennungsgebot	• Sparsamkeit bei der Datenerhebung • Getrennte Verarbeitung • Funktionstrennung zwischen Live- und Testsystem

Stand: August 2023

Comatic AG
Rathausplatz 9
6210 Sursee

Anhang B - Verzeichnis der Unterauftragsbearbeiter mit vorgängiger Genehmigung

Der Auftraggeber genehmigt, dass der Auftragnehmer folgende Unterauftragsbearbeiter je nach Bedarf der Leistung beauftragen darf:

Unterauftragnehmer	Anschrift	Zweck
ProIT Informatik AG	Freidorf 151 4132 Muttenz	Bereitstellung der ProIT-Produkte sowie Unterstützung in Support und Projekten
Microsoft Ireland Operations, Ltd.	South County Business Park Leopardstown, Dublin 18 D18 P521, Ireland	Bereitstellen der Cloud-Produkte in Microsoft Azure gem. Anhang C
METANET AG	Josefstrasse 218 8005 Zürich	Datenhosting der Produkte gem. Anhang C.

Stand: August 2023

Comatic AG
Rathausplatz 9
6210 Sursee

Anhang C - Übersicht der Cloud-Produkte mit dem jeweiligen Hoster

Produktname, Produktbereich	Hoster
Comatic as a Service (C7aas)	Microsoft
Comatic Krediscan	Microsoft
Comatic Trapo Mobile	Microsoft
Comatic Zeiterfassung	METANET

Stand: August 2023