Vereinbarung über die Auftragsdatenverarbeitung

Version 1.0.0 Thun, den 31.05.2024

A. Parteien

Verantwortlich: Kunde

Auftragsbearbeiter: Comvation AG, Burgstrasse 6, 3600 Thun, nachfolgend «Comvation»

B. Hauptvertrag

1. Diese Vereinbarung erweitert den zwischen den Parteien geschlossenen Vertrag über die für den Kunden erbrachten Dienstleistungen der Comvation («Hauptvertrag»). Sie geht dem Hauptvertrag, deren Bestandteilen und allfälligen AGB der Parteien bei Widersprüchen vor.

C. Gegenstand dieser Vereinbarung

2. Gegenstand dieser Vereinbarung ist die Bearbeitung von Personendaten im Rahmen der Erfüllung der Verpflichtungen aus dem Hauptvertrag durch Comvation. Der Hauptvertrag gilt für das rechtliche Verhältnis zwischen der Comvation AG einschliesslich sämtlicher in- und ausländischer Tochtergesellschaften und ihren Kunden

3. Gegenstand der Datenbearbeitung sind die im Hauptvertrag aufgeführten Datenkategorien, insbesondere die Folgenden: Private und berufliche Kontakt- und Identifikationsdaten, Daten zu persönlichen und Beruflichen Verhältnissen & Merkmalen, Gesundheitsdaten, Bild- und/oder Ton-Aufzeichnungen, Vertragsdaten und Auftragsdaten, IT-Nutzungsdaten, Bonitäts- und Bankdaten, Sozialdaten.

4. Gegenstand der Datenbearbeitung sind die im Hauptvertrag aufgeführten Personenkategorien, insbesondere die Folgenden: Endkunden und Interessenten des Verantwortlichen, Endkunden und Interessenten von Geschäftskunden des Verantwortlichen, Interne oder externe Mitarbeitende des Verantwortlichen, Personendaten von Kunden, Lieferanten und Partner des Verantwortlichen.

5. Die Datenbearbeitung findet an den folgenden Orten statt: Schweiz, EU, EFTA-Staaten oder Staaten, für den ein Angemessenheitsbeschluss des Bundesrats bzw. der Europäischen Kommission vorliegt.

6. Comvation ist berechtigt, zur Leistungserfüllung Unterauftragsbearbeiter einzusetzen. Comvation prüft die Unterauftragsbearbeiter sorgfältig und schliesst mit ihnen einen Auftragsdatenverarbeitungsvertrag ab, der im Wesentlichen die Bestimmungen der vorliegenden Vereinbarung enthält. Comvation gibt dem Kunden den Wechsel oder den Beizug eines neuen Unterauftragsbearbeiters im Voraus in Textform bekannt. Erhebt der Auftraggeber nicht innerhalb von **10 Tagen** nach Erhalt der Mitteilung Einsprache, gilt ein Unterauftragsbearbeiter als genehmigt.

D. Rechte und Pflichten der Parteien

7. Comvation verpflichtet sich, die bearbeiteten Personendaten zu keinen anderen als den im Hauptvertrag vereinbarten Zwecken zu verwenden. Ausgenommen hiervon ist die Bekanntgabe von Personendaten im Rahmen von behördlichen Herausgabe- oder Durchsuchungsverfügungen über welche Comvation den Kunden, falls zulässig, schnellstmöglich in Kenntnis setzt.

8. Comvation setzt bei der Durchführung der Arbeiten nur Personen oder Unterauftragsbearbeiter ein, die vertraglich oder gesetzlich zur Geheimhaltung verpflichtet und mit den relevanten Bestimmungen des Datenschutzes vertraut sind.

9. Comvation bearbeitet die Personendaten nur im Rahmen von dokumentierten Weisungen des Kunden. Mündliche Weisungen bestätigt der Kunde umgehend mindestens in Textform. Comvation weist den Kunden darauf hin, falls eine Weisung gegen geltendes Datenschutzrecht verstösst und setzt eine Bearbeitung so lange aus, bis der Kunde die Weisung in Textform bestätigt.

10. Comvation ermöglicht es dem Kunden oder einem von ihm beauftragten Prüfer, Kontrollen betr. die Einhaltung dieser Vereinbarung auszuführen. Solche Kontrollen sind mind. **10 Arbeitstage** im Voraus anzukündigen. Der Kunde hat pro Jahr einen Anspruch auf einen kostenlosen Kontrolltag. Zusätzlicher Aufwand seitens Comvation hat der Kunde zu marktüblichen Ansätzen zu vergüten.

11. Comvation stellt die Datensicherheit durch geeignete technische und organisatorische Massnahmen nach **Anlage I** sicher. Diese Massnahmen unterliegen dem technischen Fortschritt. Comvation kann alternative adäquate Massnahmen umsetzen. Dabei darf das bisherige Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert.

12. Comvation verpflichtet sich ausserdem, den Kunden innert 48 Stunden seit Feststellung über einen Vorfall betreffend die Datensicherheit zu informieren.

13. Comvation unterstützt den Kunden in zumutbarem Umfang bei der Erstellung von Datenschutz-Folgenabschätzungen für sowie zwecks Beantwortung von Gesuchen von Betroffenen und im Rahmen von Behördenanfragen oder -Kontrollen, welche die durch Comvation bearbeiteten Personendaten betreffen.

14. Kopien oder Duplikate der Daten werden ohne Wissen des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien und andere technisch notwendige Kopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenverarbeitung erforderlich sind.

15. Auf Verlangen des Kunden, spätestens aber mit Beendigung des Hauptvertrags, löscht Comvation sämtliche Personendaten des Kunden, vorbehaltlich anderweitiger Vereinbarungen (bspw. Backup-Aufbewahrung) oder gesetzlicher Aufbewahrungspflichten.

E. Dauer der Auftragsbearbeitung

16. Diese Vereinbarung bleibt so lange in Kraft, wie Comvation Personendaten des Kunden bearbeitet, d.h. ggf. über das Ende des Hauptvertrags hinaus, falls Comvation resp. deren Unterauftragsbearbeiter noch Backups mit Personendaten des Kunden aufbewahrt. In einem solchen Fall beschränkt sich das Kontrollrecht nach Ziff. 9 auf schriftliche Anfragen.

17. Diese Vereinbarung kann von Comvation jederzeit mit einer angemessenen Vorankündigungsfrist angepasst werden. Der Kunde wird in Textform darüber informiert. In

begründeten Fällen kann der Kunde dagegen Einspruch erheben. Können sich die Parteien in der Folge nicht einigen, kann Comvation den Hauptvertrag mit einer Kündigungsfrist von 30 Tagen auf einen beliebigen Zeitpunkt kündigen.

ANLAGE I – Technische und organisatorische Massnahmen

1. Vertraulichkeit

(1) Zutrittskontrolle: Der Auftragnehmer gewährleistet, dass kein unbefugter Zutritt zu Datenbearbeitungsanlagen erfolgt.

Die Zutrittskontrolle zu den Räumlichkeiten des Auftragnehmers bzw. dessen genehmigte Unterauftragnehmer, in welchen die Daten des Auftraggebers gespeichert bzw. bearbeitet oder Zugangsdaten zu den denselben gespeichert werden, gestaltet sich wie folgt:

- Schlüsselvergabe nur an beschränkten Personenkreis mit Schlüsselliste;
- Türsicherung.

(2) Zugangskontrolle:Der Auftragnehmer stellt sicher, dass keine unbefugte Systembenutzung erfolgt. Dafür ergreift er folgende Massnahmen:

- Kennwortverfahren (u.a. Komplexitätsanforderungen, Mindestlänge, regelmässiger Wechsel des Kennworts mit Historienverwaltung);
- Zwei oder Multi-Faktor Authentifizierung (gemäss Auftraggeber Voraussetzungen);
- Verwendung von zeitgesteuerter Bildschirmsperre mit Passwortschutz;
- bei Bedarf verschlüsseltes WLAN für den internen Gebrauch;
- Firewall-Einstellungen.

(3) Zugriffskontrolle:Der Auftragnehmer stellt sicher, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von den bearbeiteten personenbezogenen Daten innerhalb des Systems erfolgt. Der Auftragnehmer ergreift die folgenden Massnahmen:

- Festlegung und Kontrolle der Zugriffsbefugnisse differenziert nach Daten, Programmen und Zugriffsarten (Berechtigungskonzept);
- Zeitnahes Einspielen der notwendigen Sicherheitsupdates;
- Ständige Aktualisierung des Virenschutzes;
- Sichere Verwaltung und Verwahrung von Datenträgern/-bestände;
- Vernichtung sensibler Unterlagen oder Datenträger durch Entsorgungs-Fachbetrieb, Nachweis über Vernichtung durch Datenvernichtungsprotokoll.

(4) Trennungskontrolle: Der Auftragnehmer stellt sicher, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt bearbeitetet werden. Der Auftragnehmer ist für die Umsetzung der folgenden Massnahmen besorgt:

- «Mandantenfähigkeit» der verwendeten Software;
- Trennung der Datensätze durch Speicherung in physikalisch getrennten Datenbanken.

2. Integrität

(1) Weitergabekontrolle: Der Auftragnehmer stellt sicher, dass personenbezogene Daten bei einer elektronischen Übertragung oder einem Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Dafür ergreift er folgende Massnahmen:

- Datenvernichtung entsprechend datenschutzrechtlicher Vorgaben;
- Aufbewahrung in gesichertem Bereich;
- Archivierung aller ausgehenden E-Mails.

3. Verfügbarkeit und Belastbarkeit

(1) Verfügbarkeitskontrolle: Der Auftragnehmer stellt sicher, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust geschützt sind. Der Auftragnehmer ergreift die folgenden Massnahmen:

- Definiertes Backup-Verfahren;
- Verfügbarkeitsgewährleistung durch redundante Speichersysteme;
- Virenschutz / Firewall.

(2) Der Auftragnehmer sorgt für eine rasche Wiederherstellbarkeit der Systeme und der Daten des Auftraggebers.

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

(1) Der Auftragnehmer ist für ein angemessenes Datenschutz-Management und ein Incident-Response-Management besorgt.

(2) Der Auftragnehmer setzt datenschutzfreundliche Voreinstellungen um, damit möglichst wenig personenbezogene Daten bearbeitet werden.

(3) Auftragskontrolle: Es erfolgt keine Auftrags- bzw. Unterauftragsdatenbearbeitung ohne entsprechende Weisung des Auftraggebers. Der Auftragnehmer setzt insbesondere die folgenden Massnahmen um:

- Eindeutige Vertragsgestaltung;
- Verpflichtung der Mitarbeiter sowie von beauftragten Unternehmen (Dienstleistungsunternehmen, Steuerberater, Wirtschaftsprüfer, Sicherheitsunternehmen und weitere) zum Datenschutz und zur Geheimhaltung;
- Dokumentierte Rückgabe der ggf. überlassenen Datenträger und Löschung von Restdaten.