Vereinbarung über die **Auftragsdatenverarbeitung**

Version vom: 01.09.2023

Präambel

Der Dienstleister erbringt für den Verantwortlichen gestützt auf ein separates Vertragsverhältnis Dienstleistungen. Die vorliegende Auftragsverarbeitungsvereinbarung präzisiert die Verantwortlichkeiten der Parteien im Rahmen einer Verarbeitung von personenbezogenen Daten. Sie ergänzt diesbezüglich die aus dem Auftrag ergebenden Rechten und Pflichten zwischen der Schönenberger Gruppe (konkret Schönenberger Die Treuhänder AG, Schönenberger Die Informatiker AG, Schönenberger die Immobilienverwalter AG, Schönenberger Die Heimkompetenz, FIB schoebe AG und nachfolgend als "Auftragnehmer" bezeichnet) und dem Verantwortlichen (nachfolgend als "Auftraggeber" bezeichnet). Dieser Auftragsverarbeitungsvertrag bildet einen integralen Bestandteil der allgemeinen Geschäftsbedingungen (AGB) und ist ferner auf alle Auftragsverhältnisse zwischen dem Auftragnehmer und dem Auftraggeber anwendbar.

Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter vom Auftragnehmer oder durch ihn beauftragte Subunternehmer personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.

1. Gegenstand, Dauer, Art und Zweck der Datenverarbeitung

1.1 Die Verarbeitung beruht auf der zwischen den Parteien bestehenden Auftragsvereinbarung (im Folgenden "Hauptvertrag").

1.2 Die Art und Dauer der Verarbeitung ergibt sich aus dem Hauptvertrag und wird nach dem Prinzip von Treu und Glauben ausgeführt.

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

2. Pflichten des Auftragnehmers

2.1 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.

2.2 Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemässer Datenverarbeitung.

2.3 Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

2.4 Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit diese nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

2.5 Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

2.6 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.

2.7 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.

2.8 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.

2.9 Die Auftragsdatenverarbeitung erfolgt grundsätzlich in der Schweiz. Jegliche Verlagerung innerhalb des europäischen Wirtschaftsraums (EWR) oder in ein Drittland darf nur mit Zustimmung des Auftragsgebers und bei Einhalt der gesetzlichen Bestimmung sowie dessen Vertrages erfolgen.

3. Sicherheit der Verarbeitung

3.1 Die im Anhang 1 beschriebenen Datensicherheitsmassnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

3.2 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.

3.3 Soweit die getroffenen Sicherheitsmassnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

3.4 Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

3.5 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.

3.6 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.

4. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

4.1 Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren. Vorbehalten bleiben die gesetzlichen Aufbewahrungspflichten.

4.2 Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

5. Subordinationsverhältnisse

5.1 Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

5.2 Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen dem Auftragnehmer und dem Subunternehmer.

5.3 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.

5.4 Die Verantwortlichkeiten vom Auftragnehmer und des Subunternehmers sind eindeutig voneinander abzugrenzen.

5.5 Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Massnahmen sorgfältig aus.

5.6 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.

5.7 Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

5.8 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 vom Auftragnehmer, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

6. Rechte und Pflichten des Auftraggebers

6.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

6.2 Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen muss der Auftraggeber unverzüglich schriftlich bestätigen.

6.3 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. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.

6.4 Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen ihres Geschäftsbetriebes zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten vom Auftragnehmer, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

7. Mitteilungspflichten

7.1 Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. die Art der Verletzung;

b. soweit möglich den Zeitpunkt und die Dauer;

c. soweit möglich die Kategorien und die ungefähre Anzahl der betroffenen Personendaten;

d. soweit möglich die Kategorien und die ungefähre Anzahl der betroffenen Personen;

e. welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben und die Folgen, einschliesslich der allfälligen Risiken, zu mindern;

f. den Namen und die Kontaktdaten einer Ansprechperson.

7.2 Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstösse vom Auftragnehmer oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

7.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Massnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

8. Weisungen

8.1 Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

8.2 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.

8.3 Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

9. Weitergabe ins Ausland

9.1 Unter Umständen kann es im Rahmen der Auftragsverarbeitung auch zu Übermittlung von personenbezogenen Daten an Unternehmen im Ausland kommen. Der Auftragnehmer stellt sicher, dass diese Unternehmen im gleichen Umfang zum Datenschutz verpflichtet sind.

9.2 Entspricht das Datenschutzniveau nicht demjenigen des EWR-Raums, so nimmt der Auftragnehmer eine vorgängige Risikoeinschätzung vor und stellt vertraglich sicher, dass der gleiche Schutz wie im EWR-Raum garantiert wird. Sollte Risikoeinschätzung des Auftragnehmers negativ ausfallen, ergreift dieser zusätzliche technische Massnahmen zum Schutz der Daten.

10. Beendigung des Auftrags

10.1 Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt vom Auftragnehmer, hat dieser des nach Wahl des Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von zwei Wochen nach entsprechender Aufforderung durch den Auftragnehmer zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

10.2 Vorbehalten bleiben gesetzliche Aufbewahrungspflichten. Solche Aufbewahrungspflichten ergeben sich aus Vorschriften über das Melderecht, über die Rechnungslegung und aus dem Steuerrecht. Gemäss diesen Vorschriften müssen geschäftliche Kommunikation, geschlossene Verträge und Buchungsbelege bis zu zehn Jahren aufbewahrt werden.

10.3 Der Auftragnehmer ist verpflichtet, die unverzügliche Vernichtung bzw. Rückgabe auch bei Subunternehmern herbeizuführen.

11. Schlussbestimmungen

11.1 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit aller Verträge zwischen dem Auftragnehmer und dem Auftraggeber, unter welchen der Auftragnehmer für den Auftraggeber relevante Daten bearbeitet, sofern sich aus den Bestimmungen dieser Vereinbarung nicht länger dauernde Verpflichtungen ergeben.

11.2 In Abweichung allfälliger Schriftformvorbehalte im Hauptvertrag kann die vorliegende Vereinbarung auch auf elektronischem Weg zwischen den Parteien vereinbart oder geändert werden.

11.3 Die Pflichten aus dieser Vereinbarung gelten zusätzlich zu den im Hauptvertrag festgelegten Pflichten und schränken letztere nicht ein. In Bezug auf die in einem Anhang zu dieser Vereinbarung generisch festgelegten technischen und organisatorischen Massnahmen gehen im Widerspruchsfall die Regelungen des Vertrages vor. Im Übrigen gelten die Regelungen des Vertrages unverändert weiter.

Anhang 1- Technische und organisatorische Massnahmen

Technische und organisatorische Massnahmen

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Massnahmen zur Gewährleistung des Datenschutzes festgelegt, die der Auftragnehmer mindestens zu entrichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung der Datensicherheit, insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1. Zutrittskontrolle

Der Auftragnehmer hat die folgenden Massnahmen ergriffen, um den unerlaubten Zugriff auf IT-Systeme zu vermeiden, in denen personenbezogene Daten verarbeitet werden:

- In Rechenzentren 7/24 Überwachung mit mehrfacher Alarmsicherung
- Nur autorisierte und begleitete Zutritte zu den Rechenzentren möglich
- Kameraüberwachung über gesamtes Rechenzentrumgsgebiet
- Mehrfache Authentifizierung in Rechenzentren
- Schlüssel-Verwaltung mit manuellem Verschlusssystem (auf Schlüsselmitarbeitende beschränkte Verwendung bei Versagen des Zutrittkontrollsystems)
- Sicherheitsschlösser
- Regelmässige Überprüfung des Schlosssystems
- Besuchermanagement am Empfang
- Sorgfältige Auswahl des Reinigungspersonals

2. Zugriffskontrolle System

Der Auftragnehmer hat die folgenden Massnahmen ergriffen, um den Zugriff Unberechtigter auf Datenverarbeitungssysteme zu vermeiden:

- Vergabe von Benutzerrechten
- Zugriff nach Berechtigungskonzept gemäss Need-to-Know Prinzip
- Passwortvergabe mit Mindestanforderungen an Passwortkomplexität
- Authentifizierung mit Benutzername / Passwort und Mulitfaktor Authentifizierung
- Verwendung von Intrusion-Prevention-Systemen und von Firewalls
- Verwendung von mehreren Netzwerkzonen
- Verwendung von personalisierten Benutzerprofilen
- Einsatz von Web Application Firewalls
- Regelmässige externe Vulnerability Scans
- Patch Management
- Verwendung von Virenscannern
- Verwendung von VPN Technologie
- Verwendung eines Device-Managements
- Anzahl Administratoren auf nötiges Minimum reduziert
- Verschlüsselung transportierter Daten mit TLS
- Kontrolle der Berechtigungen bei Eintritt und Austritt von Mitarbeitenden

3. Zugriffskontrolle Daten

Der Auftragnehmer hat die folgenden Massnahmen ergriffen, um sicherzustellen, dass Nutzer nur auf diejenigen Daten Zugriff haben, für die sie autorisiert sind und um zu vermeiden, dass personenbezogene Daten ohne Autorisierungen gelesen werden können:

- Einsatz rollenbasierten Autorisierungskonzept nach Need-to-Know Prinzip
- Anzahl Administratoren auf nötiges Minimum reduziert
- Sichere Medienbereinigung vor der Wiederverwendung
- Verwendung von Schreddern
- Verschlüsselung transportierte Daten mit TLS
- Rechteverwaltung durch Systemadministratoren
- Passwort-Richtlinie mit geltenden Mindestanforderungen an Passwortkomplexität
- Sichere Aufbewahrung von mehreren Backup-Datenständen auf unterschiedlichen Speichersystemen und an mehreren Standorten
- Konforme Zerstörung von Datenträgern
- Kontrolle der Berechtigungen bei Eintritt und Austritt von Mitarbeitenden

4. Übertragungskontrolle

Der Auftragnehmer hat die folgenden Massnahmen ergriffen, um sicherzustellen, dass personenbezogene Daten nicht gelesen, kopiert oder modifiziert werden können während der elektronischen Übermittelung, des Transports oder der Speicherung:

- Verschlüsselung transportierter Daten mit TLS
- Einsatz von VPN-Verbindungen
- Dokumentation der Datenempfänger und der Übertragungszeiten
- Für den physischen Transport, sorgfältige Auswahl des Transportpersonals und der Fahrzeuge sowie Verschlüsselung des genutzten Speichermediums

5. Eingabekontrolle

Der Auftragnehmer hat die folgenden Massnahmen ergriffen, um sicherzustellen, dass es möglich ist, nachzuvollziehen und zu kontrollieren, ob und wer personenbezogene Daten eingibt, modifiziert oder aus Datenverarbeitungssystemen löscht:

- Protokollierung der Eingabe, Modifikation und Löschung von Daten
- Rückverfolgbarkeit der Eingabe, Modifikation und Löschung von Daten durch individuelle Benutzerprofile
- Rechtevergabe für Eingabe, Modifikation und Löschung von Daten basierend auf einem Autorisierungskonzept

6. Auftragskontrolle

Der Auftragnehmer hat die folgenden Massnahmen ergriffen, um sicherzustellen, dass in seinem Auftrag im Einvernehmen mit dem Verantwortlichen weiterverarbeitete Daten nur auf dessen Weisung hin verarbeitet werden:

- Sorgfältige Auswahl der Unterauftragsnehmer unter Berücksichtigung ihrer Historie (insbesondere hinsichtlich Informationssicherheit)
- Schriftliche Weisungen an Unterauftragsnehmer (über Vereinbarung der Auftragsdatenverarbeitung)
- Effektive Kontrollrechte zugesichert durch Auftragsverarbeiter
- Vorgängige Prüfung der Dokumentation und der Sicherheitsmassnahmen, die Unterauftragsnehmer ergriffen haben
- Verpflichtung der Mitarbeitenden des Auftragsverarbeiters zur Wahrung der Vertraulichkeit
- Sichere Löschung der Daten nach Vertragsende
- Fortlaufende Überwachung der Unterauftragsnehmer und deren Aktivitäten

7. Trennungskontrolle

Der Auftragnehmer hat die folgenden Massnahmen ergriffen, um sicherzustellen, dass Daten, die zu verschiedenen Zwecken erhoben wurden, separat verarbeitet werden können:

- Sicherstellung, dass Daten der Kunden/Mandanten nicht gegenseitig einsehbar sind durch logische oder physische Trennung
- Berechtigungskonzept, das die getrennte Verarbeitung der Daten anderer Kunden/Mandanten sicherstellt
- Trennung von Produktiv- und Testsystemen