Datenschutzvereinbarung und Auftragsbearbeitung

Ergänzende Vertragsgrundlage für Auftragsbearbeitungen. Gilt, soweit Sonnora Personendaten für den Auftraggeber bearbeitet. Stand 04.10.2026.

1. Zweck und Rollen

Diese Vereinbarung regelt den Umgang mit Personendaten im Rahmen des Mandats. Soweit Sonnora Personendaten ausschliesslich im Auftrag und nach Weisung des Auftraggebers bearbeitet, ist der Auftraggeber Verantwortlicher und Sonnora Auftragsbearbeiterin im Sinne des Schweizer Datenschutzgesetzes (DSG).

Soweit Sonnora Daten für eigene gesetzliche oder vertragliche Zwecke bearbeitet - insbesondere für Mandatsverwaltung, Rechnungsstellung, IT-Sicherheit, Erfüllung eigener gesetzlicher Pflichten, interne Dokumentation oder Anspruchsdurchsetzung - handelt Sonnora im hierfür erforderlichen Umfang als eigene Verantwortliche. Die Rollen richten sich nach der tatsächlichen Datenbearbeitung und nicht allein nach der Bezeichnung in diesem Dokument.

2. Gegenstand und Dauer der Auftragsbearbeitung

Gegenstand

Erbringung der im Leistungs- und Preisblatt bezeichneten Treuhand-, Buchhaltungs-, Payroll-, Abschluss-, Steuer- und Administrationsleistungen.

Dauer

Für die Dauer des Mandats zuzüglich notwendiger Übergabe-, Sicherungs- und gesetzlicher Aufbewahrungsfristen.

Bearbeitungszwecke

Mandatsausführung, Lohnverarbeitung, Buchführung, Deklarationen, Kommunikation, Dokumentation, Auswertungen und vereinbarte Behörden-/Systemprozesse.

Betroffene Personen

Insbesondere Mitarbeitende, Organe, Gesellschafter, Kunden, Lieferanten, Kontaktpersonen und wirtschaftlich berechtigte Personen des Auftraggebers, soweit für das Mandat erforderlich.

Datenkategorien

Stamm- und Kontaktdaten, Vertrags-/Geschäftsdaten, Finanz- und Buchhaltungsdaten, Lohn- und Sozialversicherungsdaten, AHV-/Sozialversicherungsnummern, Quellensteuerdaten, Aufenthalts-/Arbeitsbewilligungsdaten, Bank-/Zahlungsinformationen sowie weitere erforderliche Angaben. Je nach Mandat können besonders schützenswerte Personendaten, etwa Gesundheits-/Absenzen- oder Lohnpfändungsinformationen, betroffen sein.

3. Weisungen

Sonnora bearbeitet Auftragsdaten nur im Rahmen der dokumentierten Weisungen des Auftraggebers, der Mandatsvereinbarung und des Leistungs- und Preisblatts, ausser eine gesetzliche Pflicht verlangt eine andere Bearbeitung. Soweit rechtlich zulässig, informiert Sonnora den Auftraggeber über eine solche Pflicht.

Hält Sonnora eine Weisung für datenschutzrechtlich problematisch oder nicht umsetzbar, weist sie den Auftraggeber darauf hin und darf die betroffene Bearbeitung bis zur Klärung aussetzen.

4. Vertraulichkeit und Personal

Sonnora stellt sicher, dass Personen mit Zugriff auf Auftragsdaten zur Vertraulichkeit verpflichtet sind und nur im erforderlichen Umfang Zugriff erhalten. Mitarbeitende werden angemessen über Datenschutz und Informationssicherheit instruiert.

5. Datensicherheit

Sonnora trifft unter Berücksichtigung des Risikos, des Stands der Technik und der Art der Daten angemessene technische und organisatorische Massnahmen. Der bei Vertragsschluss geltende Mindeststandard ist in Anhang B dokumentiert und wird risikobasiert weiterentwickelt.

Der Auftraggeber ist für die Sicherheit seiner eigenen Systeme, Benutzerkonten, Endgeräte und Zugänge sowie für die rechtmässige Übermittlung der Daten an Sonnora verantwortlich.

6. Unterauftragsbearbeiter und Systeme

Der Auftraggeber erteilt Sonnora eine allgemeine Genehmigung, geeignete Unterauftragsbearbeiter und IT-Systeme einzusetzen, soweit dies für die Mandatsausführung erforderlich ist. Sonnora wählt diese sorgfältig aus und verpflichtet sie, soweit erforderlich, vertraglich zu angemessenen Datenschutz- und Datensicherheitsstandards.

Sonnora informiert den Auftraggeber über die bei Vertragsschluss vorgesehenen Unterauftragsbearbeiter und Systeme gemäss Anhang A sowie über beabsichtigte wesentliche Änderungen. Der Auftraggeber kann aus sachlich begründetem Datenschutzinteresse widersprechen. Kann keine zumutbare Alternative gefunden werden, können die Parteien den betroffenen Leistungsteil anpassen oder beenden.

Die Aufnahme eines Dienstleisters in Anhang A bedeutet nicht, dass dieser in jedem Mandat oder für sämtliche Datenkategorien eingesetzt wird. Massgebend ist die tatsächliche Nutzung im konkreten Mandat.

7. Bekanntgabe ins Ausland

Soweit Personendaten ins Ausland bekanntgegeben oder von dort aus zugänglich gemacht werden, hält Sonnora die Anforderungen des Schweizer DSG ein. Bei Staaten ohne vom Bundesrat anerkanntes angemessenes Datenschutzniveau stellt Sonnora vor der Bekanntgabe einen zulässigen Schutzmechanismus sicher, insbesondere anerkannte Standarddatenschutzklauseln oder eine andere gesetzlich zulässige Garantie bzw. Ausnahme.

Die wesentlichen Bearbeitungsstaaten und Besonderheiten der eingesetzten Systeme ergeben sich aus Anhang A. Ergänzend führt Sonnora in den Datenschutzhinweisen eine aktuelle Staaten-/Garantienübersicht. Bei cloudbasierten Diensten können technische Unterauftragnehmer in weiteren dokumentierten Staaten eingesetzt werden; soweit dadurch eine Auslandsbekanntgabe entsteht, gelten die vertraglichen und gesetzlichen Transfermechanismen des jeweiligen Dienstes.

8. Unterstützung des Auftraggebers

Sonnora unterstützt den Auftraggeber im angemessenen und für die konkrete Auftragsbearbeitung erforderlichen Umfang bei der Erfüllung datenschutzrechtlicher Pflichten, insbesondere bei Auskunfts-, Berichtigungs-, Löschungs- oder Herausgabebegehren, bei Sicherheitsvorfällen und - soweit relevant - bei Datenschutz-Folgenabschätzungen. Ausserordentlicher Aufwand kann nach vorgängiger Information verrechnet werden, soweit die Ursache nicht in einer Pflichtverletzung von Sonnora liegt.

9. Verletzungen der Datensicherheit

Sonnora informiert den Auftraggeber so rasch als möglich, nachdem sie Kenntnis von einer Verletzung der Datensicherheit erhalten hat, soweit diese Auftragsdaten betrifft. Die Mitteilung enthält die zu diesem Zeitpunkt verfügbaren Informationen, die der Auftraggeber zur Beurteilung und Erfüllung seiner gesetzlichen Melde-, Informations- und Dokumentationspflichten benötigt. Weitere verfügbare Informationen werden nachgereicht.

Sonnora dokumentiert wesentliche Sicherheitsvorfälle und unterstützt den Auftraggeber im erforderlichen Umfang bei Abklärungen und angemessenen Schutzmassnahmen.

10. Nachweise und Kontrollen

Sonnora stellt dem Auftraggeber auf angemessene Anfrage Informationen zur Verfügung, die erforderlich sind, um die Einhaltung dieser Vereinbarung zu beurteilen. Audits erfolgen grundsätzlich durch geeignete Dokumentation, Fragebögen, Prüfberichte oder Zertifizierungen.

Vor-Ort-Prüfungen können bei berechtigtem Anlass oder soweit gesetzlich erforderlich nach angemessener Vorankündigung während der Geschäftszeiten erfolgen. Vertraulichkeit, Sicherheit, Geschäftsgeheimnisse und Rechte anderer Kunden sind angemessen zu schützen.

11. Rückgabe und Löschung

Nach Ende der Auftragsbearbeitung gibt Sonnora die im Auftrag bearbeiteten Personendaten nach Wahl des Auftraggebers in einem angemessenen Format zurück oder stellt sie zur Übernahme bereit und löscht die verbleibenden Auftragsdaten, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

Daten, die Sonnora nach Mandatsende aufgrund eigener gesetzlicher Pflichten, zulässiger Dokumentationszwecke oder zur Rechtsverteidigung in eigener Verantwortlichkeit aufbewahren darf oder muss, werden nur zu diesen Zwecken weiterbearbeitet und nach Wegfall des Zwecks gelöscht. Sicherungskopien können bis zum Ablauf geregelter Backup- und Löschzyklen fortbestehen und sind während dieser Zeit gegen produktive Nutzung geschützt.

12. Verhältnis zu ausländischem Datenschutzrecht

Das Standardmandat ist auf die Schweiz ausgerichtet. Die blosse Nationalität oder der Wohnsitz einzelner betroffener Personen führt nicht automatisch zur Anwendung ausländischen Datenschutzrechts. Sollte auf eine konkrete Bearbeitung ausnahmsweise zusätzlich zwingendes ausländisches Datenschutzrecht anwendbar sein, wird vor Beginn der betreffenden Bearbeitung geprüft, ob ergänzende vertragliche oder organisatorische Massnahmen erforderlich sind.

Für Fragen der Auftragsbearbeitung geht diese Datenschutzvereinbarung bei Widersprüchen den Allgemeinen Mandatsbedingungen vor.

Anhang A - eingesetzte Dienstleister / Systeme

Stand 04.10.2026. Die Liste beschreibt die für Sonnora vorgesehenen Systeme. Der konkrete Zugriff auf Mandatsdaten richtet sich nach dem jeweiligen Einsatz.

DIENSTLEISTER / SYSTEM	ZWECK	BEARBEITUNGSORT / LÄNDER	BEMERKUNG
Comatic AG / Comatic Cloud	Buchhaltung, Payroll, ERP / Mandatsdaten	Schweiz	Comatic gibt für die Cloud zertifizierte Rechenzentren in der Schweiz an.
Infomaniak Network SA / kSuite, kDrive, Mail, Hosting	E-Mail, Kalender/Kontakte, Dateiablage, Zusammenarbeit, Hosting	Schweiz	Infomaniak gibt für Mail und kDrive Speicherung bzw. Verarbeitung in der Schweiz an.
Tresorit AG / Tresorit	Dokumentenaustausch und Dateiablage, soweit noch eingesetzt	Schweiz	Sonnora hat die Datenresidenz des verwendeten Tresorit-Tenants als Schweiz bestätigt.
Zenkit / Axonic Informationssysteme GmbH	Aufgaben/Pendenzen, Projektorganisation, ggf. kundenbezogene Metadaten	Deutschland (Frankfurt)	Zenkit gibt AWS-Rechenzentren und Backups in Deutschland an.
BlueMouse GmbH	Legacy-Hosting und E-Mail für kellertreuhand.ch	Schweiz (Zürich)	Serverstandort Zürich gemäss Anbieterangabe.
Microsoft 365 Apps / Outlook Desktop	Lokale Word-, Excel-, PowerPoint- und Outlook-Anwendungen	Lokal auf Sonnora-Endgeräten; technische Microsoft-Diagnosedaten ggf. international	Keine planmässige Ablage von Mandatsdaten in OneDrive, SharePoint oder Exchange Online. Mailkonten werden über die separat aufgeführten Mailanbieter geführt.
1Password	Passwort- und Zugangsdatenmanagement	USA (1Password.com); zusätzliche Support-/Unterauftragsbearbeitung je nach Dienst insbesondere USA, Kanada, Europäische Union und Vereinigtes Königreich	Sonnoras Account wird unter sonnoraschweizgmbh.1password.com geführt. Bei 1Password.com werden die verschlüsselten Tresordaten in den USA gehostet. Auslandbearbeitungen erfolgen nach den anwendbaren vertraglichen Transfermechanismen des Anbieters.
OpenAI Ireland Ltd / ChatGPT Business	KI-gestützte Analyse, Textentwürfe und Arbeitsunterstützung, soweit für das Mandat zulässig	Keine besondere Data-Residency-Region im Sonnora-Workspace ersichtlich; USA sowie je nach Funktion und Unterauftragsbearbeiter weitere dokumentierte Staaten	Für Sonnora ist derzeit keine besondere Data-Residency-Region dokumentiert. ChatGPT Business wird auf Basis der Business-Bedingungen/DPA genutzt. Sicherheits-/Missbrauchsverarbeitung erfolgt insbesondere in den USA; weitere mögliche Bearbeitungsstaaten sind in der aktuellen Staaten-/Garantienübersicht der Datenschutzhinweise aufgeführt. Business-Inhalte werden standardmässig nicht zum Modelltraining verwendet.

Anhang B - technische und organisatorische Mindestmassnahmen (TOM)

BEREICH	MINDESTMASSNAHMEN SONNORA
Zugriffssteuerung	Personalisierte Benutzerkonten; rollen- und aufgabenbezogene Berechtigungen; Prinzip der minimal erforderlichen Rechte; regelmässige Überprüfung und Entzug von Rechten bei Austritt oder Funktionswechsel.
Authentisierung	Starke, individuelle Passwörter; zentrale Verwaltung geschäftlicher Zugangsdaten über 1Password; Mehrfaktor-Authentisierung bei administrativen, besonders schützenswerten oder anderweitig kritischen Cloud-Zugängen, soweit technisch verfügbar.
Endgeräte	Aktuelle Betriebssystem- und Softwareupdates; aktivierter Endpoint-/Malware-Schutz; automatische Bildschirmsperre; Geräteverschlüsselung, soweit vom eingesetzten Betriebssystem unterstützt und für das Gerät vorgesehen.
Übertragung	Verschlüsselte Übertragung über TLS/HTTPS bzw. die Sicherheitsmechanismen der eingesetzten Fachsysteme; besonders schützenswerte Unterlagen werden nach Möglichkeit über dafür vorgesehene Portale/Cloud-Systeme statt ungeschützter Kanäle ausgetauscht.
Speicherung / Backups	Nutzung der Sicherungs-, Redundanz- und Wiederherstellungsmechanismen der ausgewählten Cloudanbieter; Zugriffe auf lokale Kopien werden minimiert; Wiederherstellungsmöglichkeiten werden im Rahmen der Betriebsorganisation berücksichtigt.
Mandantentrennung	Organisatorische und systemseitige Trennung von Mandaten durch Mandantenstrukturen, Ordner, Rollen und Zugriffsrechte; keine allgemeine Freigabe von Mandatsdaten an nicht zuständige Mitarbeitende.
Payroll / besonders schützenswerte Daten	Zugriff nur für zuständige Personen; Übermittlung und Speicherung in den dafür vorgesehenen Fachsystemen; besondere Zurückhaltung bei Exporten, lokalen Kopien und E-Mail-Anhängen.
KI-Nutzung	Für Mandatsdaten wird geschäftliche KI nur über freigegebene Business-Dienste eingesetzt. Eingaben werden auf das für die Aufgabe erforderliche Mass beschränkt; Passwörter und Authentisierungsgeheimnisse werden nicht eingegeben. KI-Ergebnisse werden vor fachlicher Verwendung durch Sonnora geprüft.
E-Mail / Phishing	Spam-/Malware-Schutz der Mailanbieter; Sensibilisierung für verdächtige Nachrichten; Bankverbindungs- und Zahlungsänderungen werden nicht allein aufgrund einer unbestätigten E-Mail übernommen.
Physischer Schutz	Zutritt zu Arbeitsplätzen und physischen Unterlagen nur für berechtigte Personen; Unterlagen werden ausserhalb der Bearbeitung nicht unnötig offen zugänglich aufbewahrt.
Vorfallmanagement	Sicherheitsvorfälle werden intern eskaliert, dokumentiert, eingedämmt und hinsichtlich Melde-/Informationspflichten beurteilt; betroffene Auftraggeber werden gemäss Ziff. 9 informiert.
Löschung / Aufbewahrung	Daten werden nach Mandatsende und Ablauf gesetzlicher bzw. legitimer Aufbewahrungszwecke gelöscht oder anonymisiert; technische Backups folgen den geregelten Löschzyklen der Systeme.
Dienstleister	Datenschutz- und Sicherheitsmerkmale wesentlicher Anbieter werden risikobasiert geprüft; Änderungen wesentlicher Anbieter werden dokumentiert und bei Auftragsbearbeitung gemäss Ziff. 6 kommuniziert.

Hinweis: Die TOM beschreiben den vertraglichen Mindeststandard. Interne Detailkonfigurationen, Sicherheitsinformationen und technische Geheimnisse werden aus Sicherheitsgründen nicht in diesem Kundenanhang offengelegt.