

Auftragsbearbeitungsvertrag (AVV)

SBZ Schweizer Bildungszentrum AG
Bächastrasse 75
8806 Bäch SZ
Schweiz

UID: CHE-276.629.007 MWST

Web: www.isofee.ch

E-Mail: isofee@sbz-ag.ch

Version 1.0 vom 15.10.26

Inhaltsverzeichnis

1	GEGENSTAND UND GELTUNG	3
2	ROLLEN UND WEISUNGEN	3
3	PFLICHTEN DES SBZ.....	3
4	PFLICHTEN DER KUND:INNEN.....	4
5	VERTRAULICHKEIT UND SICHERHEIT.....	4
6	UNTERAUFTRAGSBEARBEITER	5
7	BEKANNTGABE INS AUSLAND	5
8	DATENSCHUTZVERLETZUNGEN	5
9	BETROFFENENRECHTE UND UNTERSTÜTZUNG	6
10	RÜCKGABE UND LÖSCHUNG.....	6
11	NACHWEISE UND KONTROLLEN.....	7
12	VERANTWORTLICHKEIT UND HAFTUNG.....	7
13	KONTAKT UND MITTEILUNGEN	7
14	SCHLUSSBESTIMMUNGEN.....	7
15	ANHANG 1 - BESCHREIBUNG DER AUFTRAGSBEARBEITUNG	8
16	ANHANG 2 - GENEHMIGTE UNTERAUFTRAGSBEARBEITER.....	8
17	ANHANG 3 - TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN	8

1 Gegenstand und Geltung

1.1 Dieser Auftragsbearbeitungsvertrag («AVV») gilt zwischen der SBZ Schweizer Bildungszentrum AG («SBZ», «Auftragsbearbeiterin») und dem Unternehmen, das ISOfee bestellt oder nutzt («Kund:in», «Verantwortliche:r»). Er ist Bestandteil des Vertrags über ISOfee und gilt auch für kostenlose Testzugänge, soweit dabei Personendaten im Auftrag bearbeitet werden.

1.2 Der AVV regelt die Bearbeitung von Personendaten, welche Kund:innen oder deren Benutzer:innen in ISOfee eingeben, hochladen, bearbeiten oder erzeugen lassen («Kundendaten»). Die Einzelheiten ergeben sich aus Anhang 1. Für Daten, die das SBZ in eigener Verantwortung bearbeitet, insbesondere Vertrags-, Abrechnungs-, Konto-, Sicherheits- und eigene Marketingdaten, gilt die Datenschutzerklärung.

1.3 Der AVV gilt während der Nutzung von ISOfee und danach so lange, wie das SBZ Kundendaten aufbewahrt. Bei Widersprüchen zu datenschutzrechtlichen Pflichten geht dieser AVV den AGB und der Datenschutzerklärung vor. Im Übrigen bleiben die AGB anwendbar.

2 Rollen und Weisungen

2.1 Kund:innen bestimmen Zweck und Mittel der Bearbeitung, stellen deren Rechtmässigkeit sicher und bleiben gegenüber betroffenen Personen und Behörden verantwortlich. Das SBZ bearbeitet Kundendaten nur zur Vertragserfüllung, gemäss diesem AVV und aufgrund dokumentierter Weisungen.

2.2 Die Nutzung der vertraglich vorgesehenen Funktionen und Einstellungen von ISOfee gilt als dokumentierte Weisung. Zusätzliche Weisungen erfolgen in Textform. Verursachen sie Zusatzaufwand oder Änderungen an Systemen, vereinbaren die Parteien vorgängig Umsetzbarkeit, Termine und Vergütung.

2.3 Hält das SBZ eine Weisung für rechtswidrig, informiert es die Kund:innen und darf die Umsetzung aussetzen, bis die Weisung geändert oder ihre Rechtmässigkeit nachvollziehbar bestätigt wurde. Das SBZ erteilt dabei keine Rechtsberatung.

2.4 Muss das SBZ Kundendaten aufgrund zwingenden Rechts anders bearbeiten, informiert es die Kund:innen vorgängig, sofern das Gesetz dies erlaubt.

3 Pflichten des SBZ

Das SBZ verpflichtet sich insbesondere:

- Kundendaten nur für die vereinbarten Zwecke und nicht für eigene Werbung oder das Training allgemeiner KI-Modelle zu verwenden;
- nur Personen mit erforderlichem Zugriff einzusetzen und diese vertraglich oder gesetzlich zur Vertraulichkeit zu verpflichten;
- die technischen und organisatorischen Massnahmen nach Anhang 3 einzuhalten und dem Stand der Technik sowie den Risiken angemessen weiterzuentwickeln;
- die Trennung der Daten verschiedener Kund:innen sicherzustellen;
- Kund:innen bei Betroffenenanfragen, Datenschutz-Folgenabschätzungen, Konsultationen von Behörden und weiteren gesetzlichen Pflichten angemessen zu unterstützen;
- die nach diesem AVV erforderlichen Nachweise bereitzustellen;

- Kundendaten vor Vertragsende gemäss Kapitel 10 zur Sicherung bereitzustellen und nach Vertragsende zu löschen.

4 Pflichten der Kund:innen

4.1 Kund:innen stellen insbesondere sicher, dass:

- für Erhebung, Übermittlung und Bearbeitung der Kundendaten eine gültige Rechtsgrundlage besteht;
- betroffene Personen ordnungsgemäss informiert werden und erforderliche Einwilligungen vorliegen;
- Weisungen rechtmässig, vollständig und nachvollziehbar sind;
- nur erforderliche und sachlich richtige Personendaten in ISOfee bearbeitet werden;
- Benutzerkonten, Rollen und Berechtigungen aktuell gehalten sowie Zugangsdaten geschützt werden;
- benötigte Chat-Inhalte vor Vertragsende kopiert und benötigte Dokumente mit der verfügbaren Downloadfunktion heruntergeladen werden.

4.2 Die Bearbeitung besonders schützenswerter Personendaten ist nicht Gegenstand der vereinbarten Auftragsbearbeitung. Kund:innen dürfen solche Daten nicht in ISOfee eingeben oder hochladen. Sie entfernen oder anonymisieren entsprechende Informationen vor der Verwendung. Dies gilt insbesondere für Informationen aus dem Arbeitsschutz (ISO 45001) und dem Informationssicherheitsmanagement (ISO 27001), etwa Unfall-, Absenz- oder Vorfallmeldungen: Solche Informationen dürfen nur so erfasst werden, dass die betroffenen Personen nicht bestimmbar sind, insbesondere ohne Namen, Personalnummern oder andere identifizierende Merkmale. Die Verantwortung für die Anonymisierung liegt bei den Kund:innen; anonymisierte Informationen sind keine Personendaten und nicht Gegenstand dieses AVV.

4.3 Kund:innen prüfen eigenverantwortlich, ob die vereinbarten Leistungen und Massnahmen für ihre Bearbeitungsrisiken, gesetzlichen Pflichten und allfälligen Berufs- oder Geheimhaltungspflichten ausreichen.

5 Vertraulichkeit und Sicherheit

5.1 Das SBZ schützt Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme nach Massgabe des Risikos. Die vereinbarten Massnahmen sind in Anhang 3 beschrieben.

5.2 Das SBZ darf die Massnahmen ändern, wenn das Schutzniveau insgesamt nicht vermindert wird. Wesentliche nachteilige Änderungen teilt es den Kund:innen vorgängig mit, soweit dies möglich ist.

5.3 Kund:innen melden vermutete Schwachstellen, unbefugte Zugriffe und Datenschutzverletzungen unverzüglich über den publizierten Support- oder Datenschutzkontakt. Sie unterlassen eigenmächtige Sicherheitstests, welche Plattform oder andere Kund:innen beeinträchtigen könnten.

6 Unterauftragsbearbeiter

6.1 Kund:innen genehmigen dem SBZ, die aineo AG als Unterauftragsbearbeiterin beizuziehen. aineo darf ihrerseits die in Anhang 2 aufgeführten weiteren Unterauftragsbearbeiter einsetzen. Das SBZ stellt durch seinen Vertrag mit aineo sicher, dass aineo und deren Unterauftragsbearbeiter Datenschutz- und Sicherheitspflichten einhalten, die den anwendbaren Anforderungen dieses AVV entsprechen. Das SBZ bleibt gegenüber den Kund:innen für die vertragsgemässe Auftragsbearbeitung verantwortlich.

6.2 Das SBZ informiert Kund:innen mindestens 30 Tage vor dem Einsatz neuer oder ersetzter Unterauftragsbearbeiter. Dies gilt auch für Änderungen bei den von aineo beigezogenen weiteren Unterauftragsbearbeitern. Die Information erfolgt per E-Mail, über ISOfee oder über eine publizierte Liste. Kund:innen können innerhalb dieser Frist aus sachlichen Datenschutzgründen widersprechen.

6.3 Können die Parteien einen begründeten Widerspruch nicht lösen, darf das SBZ auf den betreffenden Unterauftragsbearbeiter verzichten oder den betroffenen ISOfee-Vertrag auf dessen Einsatz hin kündigen. Bereits bezahlte Gebühren für die Zeit danach werden anteilig zurückerstattet. Weitergehende Ansprüche richten sich nach den AGB.

7 Bekanntgabe ins Ausland

7.1 Ein Teil der ISOfee-Datenbearbeitung erfolgt durch OpenAI ausserhalb der Schweiz. Das betrifft den Standard-Chat, die Dokumentenerstellung sowie die Funktion «Chat mit Websuche». Die übrige Bearbeitung erfolgt durch aineo und deren weitere Unterauftragsbearbeiter in der Schweiz.

7.2 Erfolgt eine Bekanntgabe in einen Staat ohne angemessenen Datenschutz, stellt das SBZ einen zulässigen Schutz sicher, insbesondere durch anerkannte Standarddatenschutzklauseln mit erforderlichen schweizerischen Ergänzungen, oder stützt sich auf eine gesetzliche Ausnahme. Auf Anfrage informiert das SBZ über die wesentlichen Garantien.

7.3 Kund:innen weisen ISOfee nicht an, Daten in einen weiteren Staat oder an zusätzliche Empfänger:innen zu übermitteln, ohne die erforderlichen Voraussetzungen sicherzustellen.

8 Datenschutzverletzungen

8.1 Das SBZ informiert Kund:innen unverzüglich nach Bekanntwerden einer Verletzung der Datensicherheit, die Kundendaten betrifft. Die Meldung erfolgt über den vereinbarten Kontakt und enthält, soweit verfügbar:

- Art und Umfang des Vorfalls sowie betroffene Daten und Personen;
- wahrscheinliche Folgen und Risiken;
- getroffene oder vorgeschlagene Gegenmassnahmen;
- Kontaktstelle für Rückfragen.

8.2 Fehlende Informationen liefert das SBZ schrittweise nach. Es unterstützt Kund:innen angemessen bei Beurteilung, Eindämmung, Dokumentation und gesetzlich erforderlichen Meldungen. Meldungen an Behörden oder betroffene Personen nehmen Kund:innen als Verantwortliche vor, sofern das Gesetz nicht unmittelbar das SBZ verpflichtet.

8.3 Das SBZ dokumentiert Datenschutzverletzungen im gesetzlich erforderlichen Umfang. Unterstützungsleistungen werden nicht zusätzlich verrechnet, soweit das SBZ oder seine Unterauftragsbearbeiter den Vorfall verursacht haben; im Übrigen kann angemessener Zusatzaufwand verrechnet werden. Meldungen von Kund:innen über vermutete Datenschutzverletzungen sind an isofee@sbz-ag.ch zu richten. Die Bearbeitung erfolgt während der in den AGB bezeichneten Supportzeiten.

9 Betroffenenrechte und Unterstützung

9.1 Kund:innen beantworten Anfragen betroffener Personen. Erhält das SBZ eine Anfrage zu Kundendaten, leitet es diese ohne inhaltliche Beantwortung an die betreffenden Kund:innen weiter, soweit keine gesetzliche Pflicht entgegensteht.

9.2 Das SBZ unterstützt Kund:innen unter Berücksichtigung der Art der Bearbeitung und der verfügbaren Informationen bei Auskunft, Berichtigung, Löschung, Herausgabe, Übertragung, Einschränkung oder Widerspruch sowie bei Datenschutz-Folgenabschätzungen und Behördenkonsultationen.

9.3 Leistungen, die über die reguläre Bereitstellung der Plattform und zumutbare Standardauskünfte hinausgehen, darf das SBZ nach vorgängiger Information zum vereinbarten oder üblichen Ansatz verrechnen. Dies gilt nicht, soweit der Aufwand durch eine Vertragsverletzung des SBZ verursacht wurde.

10 Rückgabe und Löschung

10.1 Kund:innen sichern benötigte Kundendaten vor Vertragsende selbst. Chat-Inhalte können kopiert und Dokumente mit der verfügbaren Downloadfunktion heruntergeladen werden. Eine automatisierte oder vollständige Exportfunktion sowie die Bereitstellung in einem strukturierten Datenformat sind nicht Bestandteil der vereinbarten Leistung.

10.2 Das SBZ sperrt den produktiven Zugang nach Vertragsende und löscht oder anonymisiert produktive Kundendaten spätestens nach 90 Tagen, sofern keine gesetzliche Aufbewahrungspflicht oder dokumentierte abweichende Weisung besteht.

10.3 Sicherungskopien werden nicht selektiv verändert. Die darin enthaltenen Kundendaten bleiben geschützt, werden nicht produktiv verwendet und mit dem ordentlichen technischen Über-schreibzyklus gelöscht.

10.4 Nach Ablauf eines Testzugangs wird der Zugriff gesperrt. Die darin enthaltenen Kundendaten werden spätestens 90 Tage nach Ablauf des Testzugangs gelöscht oder anonymisiert. Für Sicherungskopien gilt Kapitel 10.3.

10.5 Soweit das SBZ Daten aufgrund zwingender Pflichten oder berechtigter Beweissicherungsinteressen länger aufbewahrt, beschränkt es die Bearbeitung auf diese Zwecke und löscht die Daten nach Wegfall des Grundes.

11 Nachweise und Kontrollen

11.1 Das SBZ stellt auf Anfrage Informationen bereit, die vernünftigerweise erforderlich sind, um die Einhaltung dieses AVV nachzuweisen. Standardisierte Nachweise, Sicherheitsinformationen oder vorhandene Prüfberichte haben Vorrang vor individuellen Kontrollen.

11.2 Reichen diese Informationen nicht aus, dürfen Kund:innen höchstens einmal jährlich eine Kontrolle durchführen oder durch eine unabhängige, fachkundige und nicht konkurrierende Stelle durchführen lassen. Voraussetzung sind ein konkreter Prüfplan, Vertraulichkeit, eine Ankündigung von mindestens 30 Tagen und die Wahrung der Sicherheit sowie der Rechte anderer Kund:innen.

11.3 Bei begründetem Verdacht auf eine wesentliche Verletzung oder nach einem erheblichen Datenschutzvorfall gelten die Beschränkungen nach Kapitel 11.2 nicht, soweit eine raschere Kontrolle erforderlich ist. Kund:innen tragen ihre Kontrollkosten und entschädigen angemessenen Zusatzaufwand des SBZ, ausser die Kontrolle weist eine wesentliche Vertragsverletzung des SBZ nach.

12 Verantwortlichkeit und Haftung

12.1 Jede Partei ist für die Einhaltung der auf sie anwendbaren Datenschutzpflichten verantwortlich. Das SBZ haftet ausschliesslich für Schäden aus einer weisungs- und vertragswidrigen Auftragsbearbeitung nach den zwingenden gesetzlichen Bestimmungen und den Haftungsregelungen der AGB.

12.2 Kund:innen tragen die Verantwortung für Rechtmässigkeit, Inhalt, Qualität und Verwendung der Kundendaten sowie für ihre Weisungen. Ansprüche Dritter und Behörden werden nach dem jeweiligen Verursachungs- und Verantwortungsanteil getragen.

13 Kontakt und Mitteilungen

Mitteilungen zu diesem AVV erfolgen in Textform an die im Vertrag bezeichneten Kontakte. Daten-
schutzanliegen und vermutete Datenschutzverletzungen können per E-Mail an isofee@sbz-ag.ch oder telefonisch unter +41 43 888 04 01 gemeldet werden. Kund:innen halten ihre administrativen und datenschutzrechtlichen Kontakte aktuell.

14 Schlussbestimmungen

14.1 Das SBZ darf diesen AVV anpassen, wenn sich Recht, Behördenpraxis, Sicherheitsanforderungen oder die Auftragsbearbeitung ändern. Wesentliche Änderungen werden mindestens 30 Tage vor Inkrafttreten angekündigt. Beeinträchtigt eine Änderung wesentliche Rechte, können Kund:innen auf den Änderungszeitpunkt kündigen.

14.2 Im Übrigen gelten die Schlussbestimmungen der AGB, insbesondere zu Textform, Teilunwirksamkeit, anwendbarem Schweizer Recht und Gerichtsstand.

15 Anhang 1 - Beschreibung der Auftragsbearbeitung

Gegenstand und Zweck: Betrieb und Bereitstellung von ISOfee; Speicherung, Organisation und Bearbeitung von Kundendaten; ISO-Systemaufbau und -pflege; Dokumentenerstellung; KI-gestützte Funktionen; Auditvorbereitung; Normrevisionen; Support, Sicherung, Fehleranalyse und Sicherheit.

Dauer: Vertragsdauer einschliesslich Testzugang sowie anschliessende Rückgabe-, Aufbewahrungs- und Löschrufen gemäss Kapitel 10.

Art der Bearbeitung: Erheben, Erfassen, Ordnen, Speichern, Anzeigen, Abrufen, Verwenden, Verändern, Verknüpfen, Übermitteln, Sichern, Wiederherstellen, Einschränken, Löschen und Anonymisieren.

Datenkategorien: Namen, geschäftliche Kontaktangaben, Funktionen und Rollen; Benutzerkennungen und Berechtigungen; technische Nutzungs-, Protokoll- und Sicherheitsdaten; Unternehmensangaben; Prozess-, Qualitäts-, Umwelt-, Risiko-, Massnahmen-, Audit- und Zertifizierungsinformationen; Eingaben, Prompts, KI-Antworten, Dokumente, Nachweise und weitere hochgeladene oder erzeugte Inhalte.

Betroffene Personen: Mitarbeiter:innen, Organe und Beauftragte der Kund:innen; Benutzer:innen von ISOfee; Kontaktpersonen bei Kund:innen, Lieferant:innen, Partner:innen und Behörden; weitere Personen, zu denen Kund:innen Daten in ISOfee erfassen.

Besonders schützenswerte Daten: Die Bearbeitung besonders schützenswerter Personendaten ist nicht vorgesehen und nicht Bestandteil der vereinbarten Leistung.

16 Anhang 2 - Genehmigte Unterauftragsbearbeiter

Direkte Unterauftragsbearbeiterin des SBZ

- **aineo AG, Schweiz:** Betrieb und technische Betreuung von ISOfee, Support sowie Koordination der für Hosting, KI und Websuche eingesetzten Dienstleister.

Weitere Unterauftragsbearbeiter von aineo

- **hosttech GmbH, Schweiz; Rechenzentren Appenzell und Nottwil:** Hosting von Anwendung, Datenbank und Dokumentenspeicher;
- **Phoenix Technologies AG («PHOENIQS»), Schweiz:** KI-Verarbeitung für Standard-Chat und Dokumentenerstellung;
- **Infomaniak Network SA, Schweiz:** KI-Verarbeitung für Standard-Chat und Dokumentenerstellung;
- **OpenAI OpCo, LLC:** KI-Verarbeitung für Standard-Chat, Dokumentenerstellung sowie die Funktion «Chat mit Websuche»; Bearbeitung ausserhalb der Schweiz, insbesondere in den USA.

17 Anhang 3 - Technische und organisatorische Massnahmen

Das SBZ und seine Unterauftragsbearbeiter setzen risikogerechte Massnahmen ein. Dazu gehören insbesondere:

- **Organisation und Vertraulichkeit:** definierte Verantwortlichkeiten, Vertraulichkeitsverpflichtungen, Sensibilisierung und geregelte Prozesse für Ein- und Austritte;
- **Zutrittskontrolle:** physischer Schutz der Rechenzentren und Betriebsstandorte sowie kontrollierter Zutritt;
- **Zugangskontrolle:** persönliche Konten, sichere Authentisierung, Passwortregeln, Sperr- und Wiederherstellungsprozesse sowie administrative Zugriffsbeschränkungen;
- **Zugriffskontrolle:** rollenbasierte Berechtigungen, Minimalprinzip, Mandantentrennung und geregelte privilegierte Zugriffe;
- **Übertragung und Transport:** verschlüsselte Netzwerkverbindungen, geschützte Schnittstellen und kontrollierte Datenübermittlungen;
- **Protokollierung:** angemessene System-, Zugriffs-, Sicherheits- und Fehlerprotokolle sowie Schutz dieser Protokolle;
- **Verfügbarkeit:** Datensicherungen, Wiederherstellungsverfahren, Systemüberwachung, Aktualisierungen und Verfahren für Betriebs- und Sicherheitsvorfälle;
- **Trennung und Löschung:** logische Trennung der Kund:innen, Trennung von Produktiv- und Testumgebungen soweit erforderlich sowie geregelte Lösch- und Entsorgungsverfahren;
- **Dienstleistersteuerung:** Prüfung, vertragliche Bindung und angemessene Überwachung von Unterauftragsbearbeitern;
- **Überprüfung:** regelmässige Beurteilung der Wirksamkeit und Anpassung an Risiken sowie technische und organisatorische Entwicklungen.