Auftragsbearbeitungsverträge und Auslandtransfers beim Einsatz von KI-Tools

Nutzt ein Unternehmen KI-Tools Dritter (z. B. Textgenerierung, Datenanalyse), liegt bei Zugriff auf Personendaten durch den Anbieter eine Auftragsbearbeitung gemäss Art. 9 DSG vor. Ein Auftragsbearbeitungsvertrag (ABV) ist zwingend notwendig, um sicherzustellen, dass der Verantwortliche die Kontrolle behält und der Anbieter die Datenschutzpflichten einhält. Wenn ein Unternehmen KI-Systeme von externen Anbietern nutzt, muss der ABV spezifische Risiken und Anforderungen berücksichtigen.

Von Lukas Lezzi, Alexandra Egger

Auftragsbearbeitung und KI-Tools

- **Zweckbindung (Art. 6 Abs. 3 DSG):** Der ABV muss klar definieren, welche Daten zu welchem Zweck bearbeitet werden. KI-Modelle dürfen nicht über den vereinbarten Zweck hinaus lernen.
- Rechte und Pflichten des Auftragsbearbeiters:
  - **Transparenz & Nachvollziehbarkeit:** Der Anbieter muss darlegen können, welche Daten zu welchem Zweck bearbeitet werden und wie die KI entscheidet (z. B. Entscheidungsbäume, regelbasierte Systeme). Weiter muss er sich verpflichten, Logs und Modellbeschreibungen zur Verfügung zu stellen.
  - **Fairness:** Um **diskriminierende Entscheide des KI-Systems zu verhindern,** soll sich der Auftragsbearbeiter verpflichten, regelmässige **Bias-Tests und Audits** durchzuführen und dem Verantwortlichen die Ergebnisse zur Verfügung zu stellen.
  - **Datensicherheit (Art. 8 DSG):** Verpflichtung des Auftragsbearbeiters zum Datenschutz-by-Design sowie zum Einführen von **technischen und organisatorischen Massnahmen** (TOMs) wie Verschlüsselung, Pseudonymisierung, regelmässigen Updates und Überwachung und Überprüfung der Modelle.
  - **Einsatz von Subunternehmern:** KI-Anbieter nutzen oft **Cloud-Dienste oder externe Datenquellen.** Der Auftragsbearbeiter darf Dritte nur mit Zustimmung des Verantwortlichen beauftragen. Alle Unterauftragsbearbeiter müssen ebenfalls DSG-konforme **Auftragsbearbeitungsverträge** abschliessen.
  - **Datenübermittlung ins Ausland:** Der ABV muss regeln, ob und wie Daten ausserhalb der Schweiz bearbeitet werden dürfen (siehe Ziff. 2).
  - Allgemeine Inhalte des ABV wie **sofortige Meldung von Datenschutzverletzungen** an den Verantwortlichen, **Unterstützungspflichten** z. B. bei Betroffenenanfragen, **Weisungsgebundenheit und Vertraulichkeit** dürfen im ABV betreffend KI-Tools ebenfalls nicht fehlen.
  - Falls **automatisierte Entscheidungen gemäss Art. 21 DSG** getroffen werden, muss sichergestellt sein, dass ein **Mensch** in den Entscheidungsprozess eingreifen kann.
  - **Pflichten nach Vertragsablauf:** Es soll vereinbart werden, dass die Daten nach **Vertragsablauf gelöscht werden** und dass **keine Kopien oder abgeleitete Daten** gespeichert bleiben.
- **Rechte und Pflichten des Verantwortlichen**
  - Der Verantwortliche ist für die Einhaltung der Datenschutzgrundsätze (gemäss Art. 6 DSG) **verantwortlich** und muss deren **Einhaltung nachweisen** können.
  - **Kontrollrechte:** Der ABV muss sicherstellen, dass Entscheidungen der KI überprüfbar und anfechtbar sind.

Auslandtransfers beim Einsatz von KI-Tools

Allgemeine Voraussetzungen

KI-Tools von Anbietern wie OpenAI, Google oder Microsoft hosten Daten oft ausserhalb der Schweiz. Gemäss **Art. 16 DSG** ist die Bekanntgabe von Personendaten ins Ausland nur zulässig, wenn ein **Angemessenheitsentscheid** des Bundesrats besteht **oder geeignete Garantien** wie **Standardvertragsklauseln (SCCs)** vorliegen, welche durch den EDÖB genehmigt oder anerkannt wurden, **oder** eine Ausnahme gemäss **Art. 17 DSG** greift (z. B. Einwilligung oder Vertragserfüllung).

Standardvertragsklauseln (SCCs)

SCCs gemäss 16 Abs. 2 lit. d DSG sind vorformulierte Verträge, welche das Mittel zur **Absicherung von Datenübermittlungen ins Ausland darstellen,** wenn **kein angemessenes Datenschutzniveau** besteht.

Für die **Schweiz** hat der **Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) die EU-SCCs vom 4. Juni 2021 offiziell anerkannt,** wobei bestimmte **Anpassungen** bzw. ein **Schweiz-Addendum** berücksichtigt werden müssen (z. B. zuständige Aufsichtsbehörde, anwendbares Recht und Gerichtsstand Schweiz). Die SCCs dürfen inhaltlich nicht verändert werden (nur ergänzende Anhänge sind erlaubt).

Die SCCs allein reichen **nicht aus,** wenn im Ausland **kein gleichwertiges Datenschutzniveau** garantiert wird, insbesondere im Hinblick auf staatlichen Zugriff auf Daten (z. B. FISA 702 oder CLOUD Act für die USA). In solchen Fällen sind **zusätzliche TOMs** wie **Ende-zu-Ende-Verschlüsselung, Pseudonymisierung vor der Übermittlung, Transparenzberichte, Transfer Impact Assessment (TIA)** erforderlich.

SCCs müssen nicht nur die allgemeinen datenschutzrechtlichen Anforderungen abdecken, sondern auch die **spezifischen Risiken im Zusammenhang mit KI** berücksichtigen. Wenn diese Punkte bereits im **ABV** geregelt sind, stellt sich die Frage, ob sie **in den SCCs nochmals geregelt werden müssen. Wenn kein Angemessenheitsentscheid vorliegt, sind SCCs zwingend.** Daher soll sichergestellt werden, dass alle datenschutzrechtlich relevanten Bestimmungen aus dem ABV **kompatibel mit den SCCs** sind. **Im Zweifel haben die SCCs Vorrang.** Um **Doppelspurigkeit** zu vermeiden, empfiehlt es sich, **in den SCCs explizit** auf den **ABV zu verweisen** oder den ABV **als Anhang in die SCC aufzunehmen.**

Transfer Impact Assessment (TIA)
Ein TIA ist im Schweizer Recht **nicht ausdrücklich geregelt,** wird aber durch die Anforderungen an geeignete Garantien (Art. 16 Abs. 2 DSG) **faktisch notwendig,** besonders bei Risikodrittstaaten wie den USA. Ein TIA prüft, welche Daten wohin übermittelt werden, welche Risiken im Ausland existieren (z. B. staatlicher Zugriff, fehlender Rechtsschutz) und welche Schutzmassnahmen bestehen bzw. ergänzt werden müssen (siehe Tabelle).

Ziel ist es, den Nachweis zu erbringen, dass der **Datenschutzstandard im Ausland «im Wesentlichen gleichwertig»** zum Schweizer Schutzniveau ist.

Regulatorische Anforderungen bei KI-Tools im regulierten Finanzmarktbereich

Wenn z. B. eine Bank ein KI-Tool nutzt, das auf einer US-Cloud läuft,

Beispielhafte Risiken und Schutzmassnahmen

Risiko	Massnahme
Zugriff durch Behörden (z. B. US-Behörden nach FISA 702 oder CLOUD Act)	▪ Datenverschlüsselung mit Schlüsselverwaltung durch ein Schweizer Unternehmen
Intransparenz der KI-Datenbearbeitung	▪ Datenschutz-Folgenabschätzung (DSFA) gemäss Art. 22 DSG ▪ Dokumentation & Auditrechte vertraglich festhalten

INFOBOX

Beim Einsatz von **KI-Tools, welche durch Dritte angeboten** werden, sollten Unternehmen immer prüfen:

- Liegt ein **Auftragsbearbeitungsvertrag (ABV)** mit dem Anbieter vor?
  - Sind die Datenschutzprinzipien (Zweckbindung, Datenminimierung, Sicherheit) gewährleistet?
  - Sind für KI-Tools relevante Risiken geregelt? (Erklärbarkeit, Fairness, Dokumentationspflicht, Einsatz von Subunternehmern)
- Werden Daten ins **Ausland** übertragen?
  - Falls ja, liegt ein **angemessenes Datenschutzniveau** vor?
  - Falls nein, sind Garantien wie **Standardvertragsklauseln** (SCCs) gemäss 16 Abs. 2 lit. d DSG, welche spezifischen Risiken im Zusammenhang mit KI berücksichtigen, vereinbart? SCCs sind **zwingend,** wenn kein angemessenes Datenschutzniveau vorliegt
- Welche **Schutzmassnahmen** gibt es? Müssen eventuell **zusätzliche Massnahmen** wie Ende-zu-Ende-Verschlüsselung, Pseudonymisierung, Transparenzberichte oder Transfer Impact Assessment (TIA) eingeführt werden?

und Kundendaten analysiert, ist dies als **Outsourcing** zu qualifizieren. Das FINMA-Rundschreiben 2018/3 «Outsourcing» ist **für alle Beaufsichtigten** der FINMA relevant und ist **zwingend zu beachten,** wenn **wesentliche Funktionen ausgelagert** werden. Dieses Rundschreiben fordert:

- **die vertragliche Regelung** der Rechte und Pflichten des Outsourcers (ähnlich wie beim ABV, aber mit zusätzlichen Anforderungen)
- das **Rechte auf Prüfung, Kontrolle und Einsichtnahme** (auch durch die FINMA)
- das Erarbeiten eines **Sicherheitsdispositivs,** das die Weiterführung der ausgelagerten Funktion in **Notfällen** erlaubt
- das Führen eines **Inventars** über die ausgelagerten Funktionen
- das **Identifizieren, Überwachen und Quantifizieren von Risiken** im Zusammenhang mit dem Outsourcing
- **die Zustimmung** des Verantwortlichen beim Suboutsourcing
- das Verbleiben der **Verantwortung** bei dervon der FINMA regulierten Unternehmung

Der Einsatz von KI-Tools durch Banken darf nicht zu einer **Verletzung des Bankgeheimnisses (Art. 47 BankG)** führen. Bei Datenübertragungen ins Ausland braucht es daher vertraglich **Geheimhaltungsverpflichtungen sowie** ggf. die **Einwilligung des Kunden,** wenn kein gesetzlicher Ausnahmetatbestand vorliegt.

Das FINIG regelt die Anforderungen an Vermögensverwalter, Trustees, Portfolioverwalter etc. Art. 9 Abs. 2 FINIG verlangt ein **angemessenes Risiko- und Kontrollmanagement.** Der **Einsatz von KI-Tools,** z. B. für Anlageberatung und Kundenanalyse, **muss in dieses Risikomanagement eingebettet werden.** Es sind Risiken des KI-Tools (z. B. Bias), das Risiko einer Datenschutzverletzung, Outsourcing-Risiken zu identifizieren, zu messen und zu steuern sowie Kontrollmechanismen (menschliche Überwachung, Logging) einzuführen.

Sowohl das FINIG als auch das FinfraG kennen Bestimmungen, welche bei einer wesentlichen Auslagerung Auditrechte für die FINMA vereinbart werden müssen.

Fazit

Beim Einsatz von **KI-Tools, welche in einem Staat,** für den kein **angemessener Schutz gewährleistet** ist, betrieben werden, **braucht es immer:**

- **einen Auftragsbearbeitungsvertrag (ABV)** mit spezifischen KI-Risiken Abdeckung (wie Nachvollziehbarkeit, Fairness) und
- **Garantien** wie z. B. **Standardvertragsklauseln (SCCs)** mit denselben spezifischen KI-Risiken Abdeckung wie beim ABV und
- **zusätzliche Schutzmassnahmen** (z. B. spezifische KI-Risiken-Abdeckung) und
- ein **Transfer Impact Assessment (TIA).**

AUTOREN

Lukas Lezzi ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.

Alexandra Egger, arbeitet als Juristin bei LezziLegal. Sie arbeitet hauptsächlich im Bereich des Datenschutzrechts.

IMPRESSUM

Verlag	WEKA Business Media AG Hermetschloostrasse 77 CH-8048 Zürich www.weka.ch
Herausgeber	Stephan Bernhard
Redaktion	Marco S. Meier
Korrektorat	Margit Bachfischer M.A., Bobingen
Layout/Satz	Tonio Schelker
Publikation	10 × jährlich, Abonnement: CHF 98.– pro Jahr, Preise exkl. MWST und Versandkosten. Als digitale Publikation erhältlich unter: www.weka-library.ch
Bildrechte	www.istockphoto.com
Bestell-Nr.	9231