Auftragsverarbeitungsvereinbarung (AVV).

Parteien

Auftraggeber (AG):

Auftragnehmer (AN):

Hauptvertrag der Parteien

Dieser AVV erweitert ihn.

Datenverarbeitung, die der AN für den AG durchführt (nur diese ist vom AVV erfasst)

Anlass/Zweck:

Betroffene Personen:

Datenkategorien:

Besondere Datenkat.:

Tätigkeit des AN:

Dauer (auch d. AVV): ☐ DSG ☐ DSGVO ☐

☐ Im Hauptvertrag geregelt: ☐ AN darf exportieren nach:

Pflichten (ansonsten gilt der Hauptvertrag)

1. Der AN verarbeitet Daten nur für Zwecke und nur auf dokumentierte Weisung des AG (z.B. Servicekonfigurationen des AG); hält er sie für unzulässig, sagt er dies dem AG.
2. Der AN sorgt stets für eine angemessene Datensicherheit gemäss geltendem Datenschutzrecht, mind. die vereinbarten TOMS. Jede Verletzung der Datensicherheit meldet er ohne Verzug mit allen Infos.
3. Der AN verpflichtet alle Hilfspersonen und Mitarbeiter zur Geheimhaltung, soweit sie dies nicht schon von Gesetzes wegen sind.
4. Der AN nutzt Unterauftragsverarbeiter nur mit Genehmigung des AG. Sie gelten ohne Widerspruch innert 30 Tagen als genehmigt. Sie sind wie der AN hier zu verpflichten.
5. Der AN exportiert keine Daten des AG ohne dessen Erlaubnis und wenn, dann nur unter Befolgung des geltenden Datenschutzrechts.
6. Der AN unterstützt den AG bei Bedarf bei der Einhaltung des Datenschutzrechts, insb. zur Erfüllung von Betroffenenrechten und bei Datenschutz-Folgenabschätzungen.
7. Nach Ende des AVV gibt der AN alle Daten zurück und löscht sie soweit ihm erlaubt.
8. Der AN weist die Einhaltung des AVV nach und der AG kann sie umfassend überprüfen.

Genehmigte Unterauftragsverarbeiter

Name	Land	Funktion

☐ Gem. sep. Liste ☐ Gemäss Website AN

Datensicherheitsmassnahmen (TOMS)

☐ Zugangskontrollen ☐ Videoüberwachung
☐ Sichere Aktenvernichtung ☐ USV
☐ Security-Checks des Personals ☐ IAM
☐ Datenzugriffe nur mit Authentifizierung
☐ MFA für alle ☐ MFA für externe Zugriffe
☐ PAM ☐ Admin nur temporär und ☑ MFA
☐ Passwortregeln ☐ Least-Privilege-Prinzip
☐ Need-to-know-Prinzip ☐ Audit-Trails
☐ Zero-Trust-Prinzip ☐ Remote nur VDI
☐ At-rest verschlüsselt ☐ In-transit versch.
☐ Endgeräte verschlüsselt ☐ TLS enforced
☐ Emails nur S/MIME ☐ ASVS Level 2
☐ Penetration Tests, ext. Security Audits
☐ ISMS ☐ Backups ☐ BCM-Konzept
☐ Firewalls ☐ IDS ☐ DLP ☐ EDR/XDR
☐ MDM ☐ HW und SW alle inventarisiert
☐ Malwareschutz ☐ akt. Patchmanagement
☐ Trennung produktive/andere Systeme
☐ Installation von Software kontrolliert
☐ Zertifizierung ISO 27001 (AVV im Scope)
☐ SOC2 Typ II Bericht ☐ SOC ☐ SIEM
☐ Weisung Informationssicherheit
☐ Schulung Informationssicherheit
☐ Gemäss separaten TOMS

Für den AG: ☐ Ersetzt früheren AVV ☐ Hat Anhänge

Name, Funktion: Name, Funktion: Datum

Für den AN:

Name, Funktion: Name, Funktion: Datum

Eine einfache Auftragsverarbeitungsvereinbarung für KMU.

Auf der vorstehenden Seite ist ein sehr einfacher Vertrag für sog. Auftragsverarbeiter (**AVV**) (oder Auftrags*be*arbeiter, wie es in der Schweiz heisst). Ein solcher Vertrag ist Vorschrift, und wer als eine für eine Datenbearbeitung verantwortliche Person keinen solchen abschliesst, kann unter dem neuen Datenschutzgesetz (**DSG**) gebüsst werden.

Profi-Auftragsverarbeiter haben ihre eigenen AVVs, die zwar für sie selbst vorteilhaft ausgelegt sind, aber für die Zwecke des Datenschutzes meistens plus/minus genügen. Oft kann dort auch gar nicht verhandelt werden. Die hier abgedruckte Vorlage ist für Fälle, in denen es keinen AVV gibt. Sie bietet das, was in einfachen Fällen nach DSG nötig und das, was als Minimum unter der EU-Datenschutz-Grundverordnung (**DSGVO**) gelten kann (wobei es sicher Leute gibt, die mehr Text sehen wollen).

Die erste Schwierigkeit besteht i.d.R. darin, eine Auftragsverarbeitung überhaupt zu **erkennen**. Sie liegt immer dann vor, wenn jemand seine eigene Datenverarbeitung durch jemand anderen machen lässt, d.h. der Auftraggeber entscheidet, was getan wird, auch wenn ihm die Dienstleister (z.B. ein IT-Service-Provider) das Menü dessen, was gewählt werden kann, vorgibt (z.B. M365, Google Analytics, eine CRM-Lösung von Salesforce, etc.). Es ist trotzdem der Kunde der wählt und es bleiben seine Daten. Typische Beispiele sind die Treuhandfirma, die Lohnausweise versendet, der Mailing-Anbieter, Firmen, die im Auftrag Daten erfassen/auswerten, IT-Service- und Cloud-Provider aller Art (aber nicht reine Telecom- oder Postdienstleister und reine Lieferanten von Hard- oder Software).

Keine Auftragsverarbeitung liegt vor, wenn der Dienstleister zwar Daten erhält, aber nur, um seinen eigentlichen Service zu erbringen, der nicht eine Datenverarbeitung ist (z.B. eine Bank, eine Versicherung, ein Berater, ein Anwalt). Dann wäre ein AVV falsch; es braucht höchstens eine Vertraulichkeitsvereinbarung ggf. mit der Pflicht, die Daten nicht anderweitig zu nutzen. Mehr zur Abgrenzung findet sich in diesen beiden Aufsätzen (für Fachleute): bit.ly/3Y4fANB, bit.ly/3ruAUQb.

Keine Auftragsverarbeiter sind nebst dem eigenen Personal auch die sonst im Betrieb integrierte und der Weisungsgewalt des Betriebs unterstellte Personen. Sie sind zur Befolgung der Weisung, zur Vertraulichkeit und zur Einhaltung der sonst geltenden Datenschutzregeln zu verpflichten und entsprechend zu überwachen.

Wer einen Auftragsverarbeiter einsetzen will, bleibt für die Verarbeitung **verantwortlich** und braucht daher nicht nur den AVV, sondern muss seinen AN sorgfältig auswählen, instruieren und überwachen.

Der AVV wird **zusätzlich zum Grundvertrag** abgeschlossen und daher ein Teil davon. Er regelt daher nur ein Minimum. So ist vorzugehen:

1. Die **Parteien** angeben; der Name reicht, da es ja schon einen Hauptvertrag gibt, wo alles drin steht (z.B. ein Service-Vertrag). Dieser ist ebenfalls zu referenzieren, z.B. mit dem Datum und der Bezeichnung.

2. Die Datenverarbeitung **beschreiben**. Falls sie im Hauptvertrag definiert ist, kann das Feld angekreuzt und die Stelle angegeben werden und der Rest leer bleiben. Sonst grob sagen, worum es geht, welche personenbezogene Daten (d.h. Daten, die einen Mensch betreffen, der identifiziert oder identifizierbar ist, keine Sachdaten) der Auftragsverarbeiter (**AN**) erhält. Besondere Kategorien sind z.B. Gesundheitsdaten und andere sensible Daten. Betroffene Personen sind jene, um deren Daten es geht. Auch angeben, ob das Schweizer DSG gilt oder auch die DSGVO (oder sonst ein bestimmtes Datenschutzrecht) und ob dem AN erlaubt ist, Daten ins Ausland zu exportieren und wohin (z.B. EWR, "weltweit"). Die "Tätigkeit" ist z.B. "Website betreiben". Die Dauer wird i.d.R. "gemäss Hauptvertrag" sein.

3. Gemäss geltendem Datenschutzrecht muss jeder für die Datenverarbeitung vom AN beschäftige **Unterauftragsverarbeiter** aufgeführt und genehmigt sein. Hierzu können die Angaben erfasst werden (z.B. "Microsoft (MIOL)", "IRL" und "Hosting", falls der AN die Microsoft Cloud für seine Lösung nutzt). Je nach Fall hat der AN eine separate Liste oder sie findet sich auf seiner Website. Dann kann das vermerkt werden.

4. Es müssen die **Massnahmen** angekreuzt werden, die der AN zum Schutz der Daten trifft (sog. **TOMS**). Das muss vor allem der AN angeben, aber der AG muss zufrieden sein, weil es um seine Daten geht. Die Vorlage nennt viele der typischen TOMS (es werden nie alle angekreuzt). Einige AN haben ihre eigenen Listen mit TOMS, dann kann auch darauf verwiesen werden.

Nicht aufgeführt sind weitere Klauseln zur Haftung, zur Beendigung oder zum geltenden Recht. Diese sind aus Sicht des Datenschutzes nicht zwingend und können vom Hauptvertrag übernommen werden. Das gilt auch für die Regelung der Kosten, die wegen des AVV entstehen können, z.B. wenn der AG Weisungen erteilt oder Unterstützung braucht.

Ist etwas unklar oder wollen Sie umfassendere Vorlagen oder Hilfe? Fragen Sie die Person Ihres Vertrauens oder dataprivacy@vischer.com.

Autor: David Rosenthal, drosenthal@vischer.com