Auftragsdatenverarbeitungsvertrag (ADV)

Datum: 31.08.2023

Dieser Vertrag versteht sich als Anhang zum aktuell gültigen Vertrag (AGB)
zwischen firm-it und ihren Partnern.

Version	Bemerkungen	Datum
1.0	Initiale Version nach revDSG	31.08.2023

Inhaltsübersicht

1. Definitionen

1 "Datensubjekt" meint eine durch bestimmte Informationen identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten verarbeitet werden. Unter Umständen können gemäss den anwendbaren Datenschutzbestimmungen auch juristische Personen als betroffene Personen gelten (so z.B. nach geltendem schweizerischem Datenschutzgesetz).

2 "Personenbezogene Daten" bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche oder juristische Person (Datensubjekt) beziehen. Eine identifizierbare natürliche Person ist eine Person, die direkt oder indirekt unter Bezugnahme auf eine Kennung wie einen Namen, eine Identifikationsnummer, Standortdaten, eine Online-Kennung oder auf eine oder mehrere physikalische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität/Identitäten identifiziert werden kann.

3 "Sensible personenbezogene Daten" meint personenbezogene Daten, die nach dem jeweils anwendbaren Recht als sensibel und/oder besonders schützenswert bezeichnet werden und/oder besonderen Kategorien zugewiesen werden. Solche Informationen können sein: Informationen über Ethnie, politische Ansichten, religiöse oder philosophische Überzeugungen, Gewerkschaftsmitgliedschaft, physische oder psychische Gesundheit, Sexualleben, ggf. tatsächliche oder mutmassliche Straftaten oder Strafen oder jede andere Information, die nach geltendem Recht als sensibel und/oder besonders schützenswert erachtet wird.

4 "Verarbeitung" bzw. "verarbeitet" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder Reihe von Vorgängen, der/die personenbezogenen Daten zum Gegenstand haben. Beispiele sind das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Archivierung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung oder Zugänglichmachen, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

5 "Datenverantwortlicher" meint die Partei, die Daten erhebt, i.e. der Partner;

6 "Auftragsverarbeiterin" meint die Partei, die Daten im Auftrag des Datenverantwortlichen erhält und verarbeitet, i.e. firm-it;

7 "Datenschutzfolgeabschätzung" bezeichnet eine Analyse betreffend die Art und Weise, wie bestimmte personenbezogene Daten gesammelt, gebraucht, geteilt, geschützt und unterhalten werden.

2. Inhalt und Dauer der Datenverarbeitung

8 firm-it fungiert im Auftrag des Partnern (Datenverantwortlicher) als Auftragsverarbeiterin und erhebt, pflegt und verarbeitet personenbezogene Daten ausschliesslich zu dem im Vertrag festgelegten Zweck und wie vom Partnern angeordnet und instruiert. Dabei müssen die Parteien die in diesem Anhang aufgeführten Datenschutz- und Sicherheitsanforderungen einhalten.

9 Sofern nicht anders vereinbart, entspricht die Dauer der Verarbeitung der Dauer des Vertrages.

10 Für firm-it als Schweizer Unternehmen, das keinen Sitz in der EU hat, gilt direkt und in erster Linie das Schweizerische Bundesgesetz über den Datenschutz.

3. Natur und Zweck der Verarbeitung

11 Von der Datenverarbeitung sind folgende Kategorien von Datensubjekten betroffen:

a. Bestehende sowie potentielle neue Klienten des Partners sowie alle Personen die diesbezüglich im Handelsregister eingetragen sind/werden (nachfolgend «Endkunden»);
b. WebApp-Nutzer des Partners.

12 Die Datenverarbeitung bezüglich Endkunden umfasst die folgenden personenbezogenen Daten:

a. Personalien (Namen, Geburtstag, Heimatort, Nationalität, Geschlecht);
b. Mobilenummer und E-Mail;
c. Ausweisdaten: Mittels OCR-Technik ausgelesen und dem Partnern in einer maschinenlesbaren Form zur Verfügung gestellt oder vom Partnern eingelieferte Daten;
d. Nationalität und Ausweistyp;
e. Akademische Titel;
f. Adressdaten;
g. Funktionen und Zeichnungsbefugnisse;
h. Foto der handschriftlichen Unterschrift und/oder beglaubigte Unterschrift;
i. Daten zum verwendeten Gerät, Browser und Zugang zum Internet (z. B. Gerätetyp, Betriebssystem, IP-Adresse, Access Provider);
j. Videoaufnahme des Vorganges der Kern-Selbstidentifikation, wobei der Ausweis und die identifizierte Person aufgezeichnet werden;
k. Fotos des amtlichen Ausweises, extrahiert aus der obengenannten Videoaufnahme;
l. Fotos des Datensubjektes, extrahiert aus der obengenannten Videoaufnahme (Selfie);

m. Daten zum verwendeten Gerät, Browser und Zugang zum Internet (z. B. Gerätetyp, Betriebssystem, IP-Adresse, Access Provider);
n. Daten über den Besuch und Aktivitäten auf den Seiten während des Identifizierungs- und/oder Signaturprozesses (wie Login mit Datum/Uhrzeit, Drücken einer «Akzeptieren»-Schaltfläche usw.);
o. Logdaten des Identifikationsvorgang (Zeitpunkt der Identifikation, Resultat der Identifikation);
p. Zertifikatsinformationen (Vorname, Name, Geburtsdatum, Ausweistyp, Ausstellungsland, Dokumentennummer, Austellungsdatum, Ablaufdatum, Mobilenummer);
q. Signierte Dokumente und/oder digital signierte Dokumente;
r. Logdaten des Signaturvorgang (Zeitpunkt der Signatur und der Ausstellung).

13 Die Datenverarbeitung bezüglich WebApp-Nutzer umfasst die folgenden personenbezogenen Daten:

a. Personalien (Namen, Geburtstag, Heimatort, Nationalität, Geschlecht);
b. Mobilenummer und E-Mail;
c. Daten zum verwendeten Gerät, Browser und Zugang zum Internet (z. B. Gerätetyp, Betriebssystem, IP-Adresse, Access Provider);
d. Logdaten der WebApp-Nutzung.

4. Verantwortlichkeiten

14 Der Partner ist in seiner Eigenschaft als Datenverantwortlicher verpflichtet:

a. die Datensubjekte über ihre Rechte betreffend Umgang mit ihren personenbezogenen Daten zu informieren;
b. die Datensubjekte über Art und Natur der personenbezogenen Daten, die im Rahmen der von firm-it bereitgestellten Dienste erhoben werden, zu informieren;
c. gemäss den geltenden datenschutzrechtlichen Bestimmungen sicherzustellen, dass eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten vorhanden ist,
d. firm-it die Kontaktdaten der Sicherheitsbeauftragten und Datenschutzbeauftragten mitzuteilen.

15 Der Partner garantiert gegenüber firm-it, dass die von firm-it zu verarbeitenden personenbezogenen Daten auf rechtmässige Weise erfasst wurden und nicht die Rechte und Freiheiten der betroffenen Person und / oder Dritter verletzen.

16 Firm-it wird in ihrer Eigenschaft als Auftragsdatenverarbeiterin:

a. die anwendbaren Datenschutzgesetze einhalten und den Partnern in wirtschaftlich angemessener Weise bei der Einhaltung der anwendbaren Datenschutzgesetze unterstützen;
b. personenbezogenen Daten nur in Übereinstimmung mit den vom Partnern dokumentierten Anweisungen und soweit dies der Vertrag erfordert verarbeiten;
c. Massnahmen ergreifen, um sicherzustellen, dass (a) Mitarbeiter, die Zugang zu personenbezogenen Daten haben, die personenbezogenen Daten nur auf Anweisung des Partnern verarbeiten, es sei denn, dies ist nach geltendem Recht, dem firm-it unterliegt, nicht zulässig; und (b) alle Mitarbeiter, die Zugang zu personenbezogenen Daten haben, sorgfältig instruiert worden sind und sich ihrerseits zur Vertraulichkeit verpflichtet haben;
d. abgesehen von einer Weitergabe an die nachstehend verzeichneten Kategorien von Subunternehmer keine Daten an wesentliche Subunternehmer weitergeben, welche zur Zeit des Vertragabschlusses nicht im Zusammenhang mit dem relevanten Service vermerkt sind und nicht nachnominiert worden sind.;
e. falls und insoweit firm-it sowie ggf. einer oder mehrere ihrer Subunternehmer die Leistungen gemäss dem Vertrag nach eigenem Ermessen ausserhalb der Schweiz bzw. der EU / des europäischen Wirtschaftsraums erbringen, im Falle von grenzüberschreitender Übermittlung von personenbezogenen Daten die Einhaltung der geltenden Datenschutzgesetze sicher stellen und, soweit gesetzlich vorgeschrieben, zusätzliche Vereinbarungen (etwa auf Basis sog. Standardvertragsklauseln der Europäischen Kommission oder durch vertraglichen Einbezug sog. Binding Corporate Rules) eingehen, die eine Absicherung eines solchen Transfers zum Gegenstand haben.
f. den Partnern unverzüglich benachrichtigen, wenn firm-it eine Anfrage oder eine Beschwerde von einem Datensubjekt erhält, mit welcher das Datensubjekt die ihm zustehenden Rechte auszuüben sucht – firm-it wird den Partnern soweit dies vernünftigerweise möglich ist darin unterstützen, auf eine solche Beschwerde oder Anfrage adäquat und zeitgerecht zu reagieren, und wird sofern dies vom Partnern genehmigt wurde: a) der betroffenen Person Zugriff auf ihre personenbezogenen Daten gestatten oder diese personenbezogenen Daten innerhalb der nach geltendem Recht festgelegten Fristen korrigieren, löschen oder blockieren; b) dem Datensubjekt alle angeforderten Informationen im Zusammenhang mit der Verarbeitung personenbezogener Daten zur Verfügung stellen; c) dem Datensubjekt personenbezogene Daten zur Verfügung stellen, die firm-it in Bezug auf das Datensubjekt besitzt, falls dies in einem allgemein

verwendeten, strukturierten, elektronischen und maschinenlesbaren Format erforderlich ist.

g. den Partnern in adäquater Weise unterstützen und mit den benötigten Informationen ausstatten, welche der Partner auf begründetes Gesuch hin vernünftigerweise benötigt, wenn er unter anderem in Bezug auf den von firm-it bereitgestellten Cloud Service gemäss anwendbarem Recht zur Durchführung einer Datenschutzfolgenabschätzung verpflichtet sein sollte.
h. dem Partnern (oder den ordnungsgemäss bevollmächtigten Vertretern oder Aufsichtsbehörden, denen der Partner unterliegt) auf begründetes Gesuch hin erlauben, die Verarbeitungsaktivitäten der firm-it im Rahmen des Vertrages (und / oder derjenigen seiner Vertreter oder Subunternehmer) daraufhin zu prüfen, ob firm-it ihre Verpflichtungen gemäss dem Vertrag und diesem Anhang in ausreichendem Masse erfüllt
i. den Partnern unverzüglich zu informieren, wenn nach Ansicht von firm-it eine der Anweisungen des Partnern gegen die Bestimmungen der geltenden Datenschutzgesetze verstösst.
j. dem Partnern jederzeit eine Kopie der personenbezogenen Daten zugehen zu lassen oder diese auf Ansuchen des Partnern zu vernichten oder zu löschen;
k. nach Beendigung des Vertrages dem Partnern alle personenbezogenen Daten zur Verfügung zu stellen und zu löschen wie im Vertrag vorgesehen.

17 firm-it kann eine angemessene Entschädigung für alle Kosten verlangen, die infolge von Gesuchen des Partners, Inspektionen, Prüfungen, Datenherausgaben und/oder weiteren unterstützenden Leistungen im Zusammenhang mit dem Datenschutz entstehen. Der Partner kann vorab zur Leistung angemessen Vorschüsse angehalten werden.

5. Datensicherheit

18 Der Partner ist für die ordnungsgemässe Verwaltung seiner Benutzerkonten verantwortlich, einschliesslich der Deaktivierung des Benutzerkontos und der Überprüfung des Kontos. Dies beinhaltet auch der sorgfältige Umgang mit Logindaten.

19 firm-it wird die Sicherheit von personenbezogenen Daten wie folgt sicherstellen:

a. firm-it implementiert geeignete technische und organisatorische Massnahmen zur Gewährleistung der Sicherheit und des Schutzes personenbezogener Daten und wird solche Massnahmen stets aufrechterhalten. firm-it berücksichtigt dabei in Übereinstimmung mit den geltenden Datenschutzgesetzen die Art und Sensibilität der zu schützenden Informationen, das von der Verarbeitung ausgehende Risiko, den Stand der

Technik und die Kosten der Implementierung und Aufrechterhaltung. Zu diesen Massnahmen gehören angemessene physische, elektronische und verfahrenstechnische Schutzmassnahmen, um die Sicherheit, Vertraulichkeit und Integrität personenbezogener Daten zu gewährleisten und insbesondere unbefugte Zugriffe und Verwendung solcher Daten zu verhindern;

b. firm-it wird die nachfolgend verzeichneten technischen und organisatorischen Massnahmen etablieren und aufrechterhalten.

c. firm-it wird den Partnern so bald wie möglich benachrichtigen, wenn ihr bekannt wird oder sie den begründeten Verdacht hat, dass (a) unbefugte Zugriffe auf oder eine unbefugte Nutzung von personenbezogenen Daten stattgefunden haben, die die Sicherheit, Vertraulichkeit oder Integrität personenbezogener Daten gefährdet; oder (b) Systeme, die personenbezogene Daten enthalten, in einer Art und Weise kompromittiert worden sind, die zu unbefugtem Zugriffen geführt haben («Data Security Breach»).

d. Im Falle eines Data Security Breach (a) muss der Verstoss gegen die Datensicherheit von firm-it unverzüglich untersucht, korrigiert, mitigiert, behoben und anderweitig behandelt werden, indem personenbezogene Daten, die von einem Data Security Breach betroffen sind, identifiziert und ausreichende Massnahmen ergriffen werden, um die Fortsetzung der akuten Gefährdung zu verhindern und künftigen Gefährdungen vorzubeugen; und (b) wird firm-it dem Partnern sämtliche Informationen und jede vernünftige Unterstützung zukommen lassen, soweit die nützlich und erforderlich ist, damit der Partner den Data Security Breach bewerten und gegebenenfalls adäquat und in Übereinstimmung mit den massgeblichen Datenschutzgesetzen über eine Datenschutzverletzung informieren kann.

6. Subunternehmer

20 Die zur Vertragserfüllung zugezogenen Subunternehmer werden verpflichtet, die anwendbaren gesetzlichen Bestimmungen einzuhalten.

21 Firm-it kann in nachfolgend genannten Fällen Subunternehmer zu Erfüllung der Leistungen beiziehen.

22 Zur Nutzung der WebApp im Allgemeinen:

a. IT-Entwicklung und Support;

b. Hosting der verwendeten Applikationen;

c. Betrieb und Wartung der Server;

d. Datenbanken wie CRM;

e. E-Mail & Newsletter Versand sowie Monitoring;
f. Rechtsdienstleister;
g. Validierungsanbieter.

23 Zur Leistungserbringung bei Produkt A+B im Besonderen:
a. Urkundspersonen;
b. Stellvertretungen im Beurkundungsprozess.

24 Zur Nutzung der eSignatur im Besonderen:
a. Signaturplattformen;
b. eSignatur-Dienstleister;
c. Identifikationsdienstleiter (insb. AutoIdent);
d. Kommunikationsdienstleister zwecks verschlüsselter Übermittlung (insb. an die Handelsregisterämter);
e. E-Mail Versand und Monitoring;
f. Authentifizierung von QES;
g. Zulassungsbestätigungen (aktuell Cygillum).

25 Die vorstehende Auflistung wird fortlaufend aktualisiert.

7. Technische und organisatorische Massnahmen

26 Nachstehend wird dargelegt, welche technischen und organisatorischen Massnahmen umgesetzt wurden, um den Datenschutz-Anforderungen zu genügen.

27 Zugangskontrollen: Unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren.

28 Massnahmen Büroräume: Der Zutritt zu den Büroräumen erfolgt mittels persönlichen Badges oder über ein Schliesssystem mit in den Schlüsseln integrierten Chipkarten. Die Türen sind ausserhalb der Bürozeiten verschlossen.

29 Massnahmen Data Center: Die Data Center sind gegen unbefugten Zutritt gesichert. Der Zutritt zum Data Center wird über ein überwachtes Zugangssystem gesteuert.

30 Personendatenträgerkontrolle: Unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen.

31 Massnahmen: firm-it erlaubt den Einsatz von Personendatenträgern nicht.

32 Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können.

33 Massnahmen: Nur dem Partner werden die erhobenen Personendaten zur Verfügung gestellt. Nach einer Frist von maximal 90 Tagen werden die Ausweiskopien auf der WebApp gelöscht.

34 Speicherkontrolle: Unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern.

35 Massnahmen: Der Schreibzugriff ist auf die Systemadministratoren technisch beschränkt. Lesezugriffe auf System-Ebene haben nur die entsprechenden Support-Mitarbeitenden.

36 Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen.

37 Massnahmen: firm-it verfolgt standardmässig den Least-Privilege Ansatz, so dass sämtliche Mitarbeiter nur die Rechte bekommen, welche sie zur Erfüllung ihrer Arbeit benötigen.

38 Eingabekontrolle: In automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.

39 Massnahmen: Der Endkunden gibt seine Personendaten selber ein, im Kernschritt Selbstidentifikation werden die Daten aus dem Ausweis maschinell ausgelesen und dann im Verifikationsschritt durch einen RA-Agenten überprüft und sofern notwendig korrigiert. All dies ist über die Logs nachvollziehbar.

40 Der Partner wird künftig zudem Daten via die API's einliefern können. Der Authentifizierung erfolgt mittels API Token. Das Einliefern der Daten ist über die Logs nachvollziehbar.

* * * * * * *