AUFTRAGSDATEN

BEARBEITUNGSVEREINBARUNG

(ADV)

AUFTRAGSDATENBEARBEITUNGSVEREINBARUNG (ADV)

durch die IDP Treuhand AG und ihrer verbundenen Unternehmen (nachfolgend IDP) [Stand 01.09.2023]

Die vorliegende Auftragsdatenbearbeitungsvereinbarung (ADV) konkretisiert die Verpflichtungen der Parteien hinsichtlich der Vorgaben des Schweizer Datenschutzgesetzes (DSG). Die Vereinbarung ergänzt in Bezug hierauf den Mandatsvertrag/die Mandatsverträge zwischen der IDP und dem Kunden.

Die ADV gilt nur sofern und soweit die nachfolgenden Voraussetzungen kumulativ erfüllt sind:

1) Der Kunde ist Verantwortlicher oder Auftragsdatenbearbeiter im Anwendungsbereich des DSG und
2) die IDP wird im Rahmen des Mandatsvertrages als Auftragsdatenbearbeiter oder Unter-Auftragsdatenbearbeiter für die Bearbeitung von Personendaten bzw. von personenbezogenen Daten, die vom Anwendungsbereich des DSG erfasst sind (nachfolgend relevante Personendaten), herangezogen.

Gegenstand, Art und Zweck, Dauer der Bearbeitung

Gegenstand, Art und Zweck sowie Dauer der Bearbeitung ergeben sich aus dem Mandatsvertrag. Die Kategorien betroffener Personen, die Kategorien der zu bearbeitenden relevanten Personendaten sowie die zu treffenden technischen und organisatorischen Massnahmen (nachfolgend TOM) sind im Anhang zu dieser ADV aufgeführt.

Anwendungsbereich und Verantwortlichkeit

Die relevanten Personendaten werden durch die IDP ausschliesslich zum Zwecke der Vertragserfüllung bzw. zu den im Mandatsvertrag vereinbarten Zwecken bearbeitet.

Für die Rechtmässigkeit der Datenbearbeitung an sich, inklusive der Zulässigkeit der Auftrags-/Unter-Auftragsdatenbearbeitung, ist alleine der Kunde verantwortlich. Die IDP kann davon ausgehen, dass ihr übertragene Aufträge zur Datenbearbeitung zulässig sind.

Die Weisungen des Kunden sind in dieser ADV sowie dem Mandatsvertrag dokumentiert. Der Kunde kann der IDP darüberhinausgehende Weisungen in Bezug auf die Bearbeitung der relevanten Personendaten schriftlich erteilen. Die IDP wird diesen Weisungen nachkommen, sofern diese im Rahmen der vertraglich vereinbarten Leistungen durch die IDP umsetzbar und objektiv zumutbar sind. Sind die Weisungen mit Mehrkosten für die IDP verbunden oder führen zu einem geänderten Leistungsumfang, so stellen diese eine Vertragsanpassung/-erweiterung dar mit entsprechenden Kostenfolgen für den Kunden.

Wenn die IDP der Auffassung ist, dass eine Weisung des Kunden gegen das DSG verstösst, informiert sie den Kunden unverzüglich. In diesen Fällen kann die IDP die Umsetzung der Weisung aussetzen, bis sie vom Kunden bestätigt oder abgeändert wurde. Bei Weisungen des Kunden im Zusammenhang mit der Vergabe von Zugriffsberechtigungen oder der Herausgabe von relevanten Personendaten an den Kunden selbst darf die IDP jederzeit davon ausgehen, dass diese Weisungen gesetzeskonform sind. Die IDP kann jedoch vom Kunden eine schriftliche Bestätigung verlangen; sie ist dazu aber nicht verpflichtet.

Pflichten der IDP

Die Bearbeitung relevanter Personendaten durch die IDP erfolgt ausschliesslich basierend auf den Bestimmungen aus dem Mandatsvertrag und dieser ADV – vorbehältlich der Erfüllung gesetzlicher, regulatorischer oder behördlicher Verpflichtungen durch die IDP.

Die IDP wird die im Anhang zu der vorliegenden ADV definierten TOMs zum Schutz der relevanten Personendaten treffen. Die IDP kann die vereinbarten TOMs ohne Rücksprache mit dem Kunden jederzeit anpassen, solange die Gesetzgebung zum Datenschutz (DSG) auch weiterhin eingehalten wird.

Die IDP führt ein Verzeichnis der Bearbeitungstätigkeiten. Dem Kunden kann auf Anfrage hin Einblick in diejenigen Teile dieses Verzeichnis gewährt werden, die direkt von der Leistungserbringung durch die IDP gegenüber dem Kunden betroffen sind.

Den mit der Bearbeitung der relevanten Personendaten des Kunden betrauten Mitarbeitenden und weiteren Hilfspersonen der IDP ist es untersagt, die relevanten Personendaten zu anderen Zwecken als den im Mandatsvertrag genannten und in Abweichung zu dieser ADV zu bearbeiten. Die IDP stellt weiter sicher, dass sich die zur Bearbeitung der relevanten Personendaten betrauten Personen zur Vertraulichkeit verpflichten und/oder angemessenen gesetzlichen Verschwiegenheitspflichten unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht nach Beendigung des Mandatsvertrages unverändert fort.

Bei Bekanntwerden von Verletzungen des Schutzes der relevanten Personendaten bei der IDP oder einem Unter-Auftragsdatenbearbeiter der IDP wird der Kunde unverzüglich in Kenntnis gesetzt. Die Information erfolgt schriftlich, wobei die Schriftlichkeit per E-Mail ausreichend ist. Der Kunde wird über Art und Ausmass der Verletzung und möglicher Abhilfemassnahmen informiert. In einem derartigen Fall sprechen sich die Parteien unverzüglich ab und treffen die erforderlichen Massnahmen zur Sicherstellung des Schutzes der relevanten Personendaten sowie zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und die Parteien.

Ansprechpersonen in Bezug auf den Datenschutz können unter datenschutz@idpag.ch erreicht werden.

Das Verfahren betreffend Rückgabe bzw. Löschung von relevanten Personendaten bei Vertragsende erfolgt basierend auf den vertraglichen Bestimmungen. Die IDP gibt diese dem Kunden zurück, löscht diese im zumutbaren und technisch möglichen Rahmen oder archiviert die Daten gemäss den gesetzlichen Aufbewahrungsbestimmungen. Für die Löschung relevanter Personendaten setzen die IDP resp. Ihre Unter-Auftragsdatenverarbeiter etablierte Verfahren ein.

Pflichten und Obliegenheiten des Kunden

Im Verantwortungsbereich des Kunden (bspw. auf eigenen Systemen, Applikationen/Umgebungen) trifft dieser eigenständig angemessene technische und organisatorische Massnahmen (TOM) zum Schutz der relevanten Personendaten.

Sofern der Kunde im Rahmen der Leistungserbringung durch die IDP Verletzungen in Bezug auf datenschutzrechtliche Bestimmungen feststellt, informiert er die IDP unverzüglich.

Für die im Rahmen des Auftrages anfallenden Datenschutzfragen sowie in Fällen, in welchen der Kunde einen Datenschutzberater zu ernennen hat, teilt der Kunde der IDP die Ansprechpersonen mit.

Anfragen betroffener Personen

Sofern betroffene Personen direkt an die IDP gelangen mit Anfragen/Forderungen zur Auskunft, Löschung, Berichtigung oder anderweitiger Ansprüche hinsichtlich relevanter Personendaten, wird die IDP die betroffene Person an den Kunden verweisen. Dies unter dem Vorbehalt, dass die Informationen seitens der betroffenen Person für eine Zuordnung an den entsprechenden Kunden ausreichend sind.

Die IDP unterstützt den Kunden auf Wunsch und gegen Vergütung im Rahmen ihrer Möglichkeiten bei der Erfüllung der Pflichten gegenüber der betroffenen Person (insbes. Lösch- und Auskunftsbegehren). Weiter bietet die IDP gegen Vergütung zusätzliche Unterstützungen beispielsweise bei einer Datenschutzfolgeabschätzung oder bei Meldungen und Konsultationen mit Aufsichtsbehörden an.

Nachweismöglichkeiten und Audits

Der Kunde kann auf eigene Kosten datenschutzrechtliche Audits anfragen. Die datenschutzrechtlichen Audit-Rechte sind jeweils durch anerkannte Prüfstellen vorzunehmen. Der Grundsatz der Verhältnismässigkeit sowie die schutzwürdigen Interessen der IDP (u.a. an Geschäftsgeheimnissen und Geheimhaltung) sind angemessen zu berücksichtigen. Sämtliche Kosten im Zusammenhang mit derartigen Audits, inklusive der internen Kosten der IDP im Zusammenhang mit dem Audit (u.a. Mitwirkung), sind vollständig durch den Kunden zu tragen.

Ergeben sich aus einem Audit Verletzungen der vorliegenden ADV oder Mängel in der Umsetzung der Pflichten der IDP, so hat die IDP unverzüglich geeignete und zumutbare (Korrektur-)Massnahmen umzusetzen.

Benutzung von Unter-Auftragsdatenbearbeitern, Beizug von Dienstleistern

Die IDP ist zum Beizug von Unter-Auftragsdatenbearbeitern berechtigt. Dafür wird die IDP mit ihren Unter-Auftragsdatenbearbeitern geeignete Vereinbarungen treffen.

Die IDP ist zum Beizug von Unter-Auftragsdatenbearbeitern berechtigt, sofern diese mindestens die gleichen technischen und organisatorischen Massnahmen einhalten. Die für die Auftragsbearbeitung verwendete IT-Systeme werden von verschiedenen Anbietern bereitgestellt und betreut. Diese beinhalten auch die Durchführung von Wartung und Systembetreuungsarbeiten. Mit allen Dienstleistern, die möglicherweise Einsicht in Personendaten haben könnten, trifft die IDP vertragliche Vereinbarungen.

Externe IT-Dienstleister, Cloud-Provider

Die IDP kann im Rahmen der Erbringung der Dienstleistungen auf externe IT-Dienstleister und auf Cloud-Provider mit Servern in der Schweiz zurückgreifen und bestimmte IT-Dienstleistungen sowie Kommunikationsmittel einsetzen, welche mit Datensicherheitsrisiken verbunden sein können (z.B. E-Mail, Microsoft 365, Zoom). Dem Kunden obliegt es, die IDP zu informieren, wenn sie besondere Sicherheitsmassnahmen wünscht (z.B. Verschlüsselung bei E-Mail-Kommunikation). Ohne anderslautende Instruktionen ist die IDP insbesondere berechtigt, unverschlüsselt per E-Mail zu kommunizieren.

Bekanntgabe ins Ausland

Die IDP achtet darauf, Personendaten grundsätzlich und nach Möglichkeit innerhalb der Schweiz zu bearbeiten. Der Kunde ist sich jedoch bewusst, dass IDP handelsübliche Software benützt, bei welcher ein

Datenverkehr ins Ausland unvermeidlich ist. Jede Bekanntgabe von relevanten Personendaten durch die IDP ins Ausland ist zulässig, wenn die IDP die vorerwähnten datenschutzrechtlichen Bestimmungen einhält. Soweit eine derartige Bekanntgabe von relevanten Personendaten vom Kunden gewünscht bzw. in seinem Auftrag erfolgt, obliegt die Einhaltung der einschlägigen Bestimmungen ausschliesslich dem Kunden.

Schlussbestimmungen

Die vorliegenden ADV kann in Abweichung zu allfälligen Schriftformabreden/-vorbehalten im Mandatsvertrag auf elektronischem Wege vereinbart werden.

Die Rechte und Pflichten aus der ADV gelten ergänzend zum Mandatsvertrag. Die Regelungen des Mandatsvertrages gelten unverändert weiter. Im Widerspruchsfalle gehen die Regelungen des Mandatsvertrages vor. Der Kunde hat Kenntnis von der Datenschutzerklärung der IDP.

ANHANG – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

Daten – verwendete Datenelemente

1. Basierend auf den Verträgen überlässt der Kunde der IDP in seinem Ermessen und in seinem Auftrag Personendaten sowie ggfs. geheimnisgebundene Daten zur Bearbeitung.
2. In Bezug auf Personendaten gilt es zwischen Personendaten und besonders schützenswerten Personendaten zu unterscheiden.
    - Personendaten: Als Personendaten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.
    - Besonders schützenswerte Personendaten: Unter besonders schützenswerten Personendaten sind heikle Personendaten zu verstehen, deren Bearbeitung besonderen Anforderungen unterstehen kann. Zu den besonders schützenswerten Personendaten zählen bspw. Daten über verwaltungs- und strafrechtliche Sanktionen, Gesundheitsdaten, biometrische Daten, sowie Daten über Massnahmen der sozialen Hilfe
3. Die Datenbearbeitungen der IDP können insbesondere folgende Personen betreffen:
    - Potentielle Kunden, Kunden, Geschäftspartner – welche natürliche Personen sind
    - Angestellte von Kunden (MitarbeiterInnen), welche beim Kunden auf der Lohnliste geführt sind
    - MietinteressentInnen und MieterInnen in Objekten der Kunden
    - Versicherte Personen, die der Vorsorgelösung des Kunden angehören
    - Drittpersonen, die mit denjenigen Personen, die dem Kunden / dem Arbeitgeber / der Vorsorgelösung des Kunden angehören, (rechtlich) verbunden sind

    Dabei kann es sich um folgende Arten von Personendaten handeln:
    - Stammdaten (u.a. Vorname, Nachname, Geburtsdatum, Alter, Geschlecht, Zivilstand, Nationalität)
    - Finanzdaten (u.a. Lohn, Altersguthaben)
    - Vertrags- bzw. Leistungsdaten
    - Gesundheitsdaten
    - Angaben zur sozialen Hilfe oder straf- und verwaltungsrechtlichen Sanktionen
    - Kommunikationsdaten (Telefon, E- Mail etc.)
4. Bei geheimnisgebundenen Daten kann es sich u.a. um Daten handeln, die dem Berufsgeheimnis, dem Bankgeheimnis oder der Verschwiegenheitspflicht gemäss Sozialversicherungsrecht unterliegen.
5. Die Vereinbarung über die Auftragsdatenvereinbarung ist nicht anwendbar auf Daten, welche durch den Kunden verschlüsselt wurden und für die IDP nicht lesbar/einsehbar sind.
6. Nachfolgend werden die durch die IDP implementierten technischen und organisatorischen Massnahmen zum Schutze der anvertrauten Daten (besonders schützenswerte Personendaten und/oder geheimnisgebundene Daten) beschreiben. Die Beurteilung der Angemessenheit dieser Massnahmen obliegt ausschliesslich dem Kunden.

Technische und organisatorische Massnahmen

Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, mit denen die Verarbeitung durchgeführt wird und mit denen Daten bearbeitet werden.

Die Zugangskontrolle erfolgt durch:

- Abgeschlossene Bereiche
- Schliesssystem mit zugehöriger Schlüsselliste (Schliessplan)
- Auswahl von Mitarbeitenden unter Sorgfaltspflichtpunkten (insbesondere berufliche Fähigkeiten und Integrität)

Datenträgerkontrolle

Die Datenträgerkontrolle soll verhindern, dass Unbefugte Datenträger lesen, kopieren, verändern oder löschen können.

Die Datenträgerkontrolle erfolgt durch:

- Datenträger werden sicher aufbewahrt in separaten, verschlossenen Räumlichkeiten
- Einsatz Standleitungen resp. VPN-Tunnel
- Die Datenweitergabe erfolgt grds. in anonymisierter oder pseudonymisierter Form an Dritte. Je nach Bearbeitungszweck sind jedoch anonymisierte Formen nicht möglich resp. praktisch nicht nutzbar, in diesen Fällen erfolgt eine Weitergabe stets in verschlüsselter Form.
- Datenträger werden stets ordnungsgemäss durch einen auf Aktenvernichtung spezialisierten Dienstleister vernichtet
- Physische Akten werden stets durch einen auf Aktenvernichtung spezialisierten Dienstleister vernichtet

Speicherkontrolle

Die Speicherkontrolle soll verhindern, dass Unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, verändern und löschen können.

Die Speicherkontrolle erfolgt durch:

- Festlegung von Berechtigungen in den IT-Systemen
- Wo sinnvoll und möglich differenzierte Berechtigungen für lesen, löschen und ändern
- Wo sinnvoll und möglich differenzierte Berechtigung für Daten, Anwendungen und Betriebssystem
- Rechteverwaltung ausschliesslich durch Systemadministrator
- Die Anzahl der Administratoren wird stets auf das Notwendigste reduziert
- Passwortrichtlinien
- Protokollierung von Zugriffen auf Anwendungen (mindestens bei datenschutzrechtlich relevanten und heiklen Vorgängen)

Benutzerkontrolle

Die Benutzerkontrolle soll verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzen können.

Die Benutzerkontrolle erfolgt durch:

- Festlegung zugangsberechtigter Mitarbeiter
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername/Passwort oder 2-Weg-Authentifizierung
- Sporadische Kontrolle von Berechtigungen
- Sperrung von Berechtigungen ausscheidender involvierter Personen

- Zuordnung von Benutzerprofilen zu IT-Systemen, Datenbanken etc. wo sinnvoll und möglich
- Einsatz von Anti-Viren-Software und Firewalls
- Einsatz von Verschlüsselungs-Technologie

Zugriffskontrolle

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschliesslich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Die Zugriffskontrolle erfolgt durch:

- Festlegung von Berechtigungen in den IT-Systemen
- Wo sinnvoll und möglich differenzierte Berechtigungen für lesen, löschen und ändern
- Wo sinnvoll und möglich differenzierte Berechtigung für Daten, Anwendungen und Betriebssystem
- Rechteverwaltung ausschliesslich durch Systemadministrator
- Die Anzahl der Administratoren wird stets auf das Notwendigste reduziert
- Passwortrichtlinien
- Protokollierung von Zugriffen auf Anwendungen (mindestens bei datenschutzrechtlich relevanten und heiklen Vorgängen)

Übertragungs- und Transportkontrolle

Die Übertragungs- und Transportkontrolle soll gewährleisten, dass bei der Übermittlung personenbezogener Daten und beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt bleiben sowie überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Die Übertragungs- und Transportkontrolle erfolgt durch:

- Einrichtung von Standleitungen bzw. Verschlüsselungstechnologien
- MS 365, dieses wird soweit möglich von einem Schweizer Partner bezogen, womit die Datenhaltung in der Schweiz (unter Beachtung der Standardvertragsklauseln seitens MS) nach bestem Wissen und Gewissen sichergestellt ist.
- Mobile Datenträger werden nach Stand der Technik verschlüsselt
- Bei E-Mail, Cloud-Plattformen: Transportverschlüsselung und Inhaltsverschlüsselung bei besonders schützenswerten personenbezogenen Daten nach Stand der Technik.
- Bei E-Mail: sämtliche Mails werden mit einer digitalen Signatur versehen
- Homepage: diese wird mittels SSL-Zertifikat verschlüsselt (sichere Verbindung)

Wiederherstellbarkeit

Die Wiederherstellbarkeit soll gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Die Wiederherstellbarkeit erfolgt durch:

- BackUp-Prozess unter Nutzung eines externen spezialisierten Dienstleisters
- Periodische stichprobenweise Prüfung der Wiederherstellung
- Physische Akten sicher in abschliessbaren Räumlichkeiten verwahrt

Zuverlässigkeit

Die Zuverlässigkeit soll gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Die Zuverlässigkeit wird erreicht durch:

- Einsatz von Anti-Viren-Schutz und Firewalls

- BackUp-Prozess
- Awareness der Mitarbeiter
- Laufende Updates

Datenintegrität

Die Datenintegrität soll gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Die Datenintegrität erfolgt durch:

- BackUp-Prozess unter Nutzung eines externen spezialisierten Dienstleisters

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Die Verfügbarkeitskontrolle erfolgt durch:

- Unterbrechungsfreie Stromversorgung durch Notstrombatterie (zeitlich begrenzt)
- Geräte zur Überwachung der Temperatur und Feuchtigkeit im Serverraum
- Feuerlöschgerät
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort (spezialisierter Dienstleistungsanbieter)