Auftragsverarbeitungsvertrag

Vertrag zur Auftragsverarbeitung

zwischen

elopay GmbH
Skalitzer Straße 138
10999 Berlin

als Auftragsverarbeiter (hier bezeichnet als elopay oder wir)

und

Martina Baehr, Projektmanagement plus
Stettiner Str. 4
51469 Bergisch Gladbach

als Verantwortlicher (hier bezeichnet als „Kunde“ oder du)

Präambel

Elopay bietet dir mit elopage.com die perfekte Plattform, um deine digitalen Produkte & Online-Kurse schnell und unkompliziert zu erstellen und optimal zu verkaufen. elopage vereint die wichtigsten Komponenten auf einer Plattform und hilft dir, effizienter und schneller zu wachsen. Unsere Plattform elopage.com enthält: Alle wichtigen Bezahlarten, Content-Auslieferung, Kunden- und Nutzermanagement, Kurs- und Mitgliederbereiche und automatisierte Prozesse, wie die Rechnungserstellung und Steuerberechnung. Unser App-Store bietet weitere Verknüpfungen und Optionen.

Du möchtest elopay mit den in § 2 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung.

Damit wir diese Vorgaben einhalten, schließen wir mit dir den folgenden Vertrag:

1 Wichtige Begriffe

Damit du diesen Vertrag besser verstehst klären wir zunächst einmal die wichtigsten Begriffe: (1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

D.h. jeder der elopage und die zur Verfügung gestellten Leistungen nutzen möchte ist „Verantwortlicher“. Um die Leistungen von elopage nutzen zu können, ist es erforderlich, dass personenbezogene Daten der Kunden von dir auf der Plattform von elopage verarbeitet werden können.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Du entscheidest selbst, welche Leistungen du von elopay im Einzelnen in Anspruch nehmen möchtest. In Anlage 1 sind unsere Leistungen aufgelistet. Elopay verarbeitet dann in deinem Auftrag die Daten, um dir Analysen etc. zur Verfügung stellen zu können.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(5) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

2 Vertragsgegenstand

(1) Wir erbringen für dich Leistungen im Bereich E-Commerce auf der Grundlage unserer Allgemeinen Geschäftsbedingungen in der jeweils aktuellen Fassung. („Hauptvertrag“). Dabei erhalten wir Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung von dir.

Umfang und Zweck der Datenverarbeitung durch uns ergeben sich immer aus dem Hauptvertrag und den Leistungen, die du in Anspruch nimmst. Dem Kunden obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Um die datenschutzrechtlichen Rechte und Pflichten zwischen dir und uns zu regeln, wird dieser Auftragsverarbeitungsvertrag geschlossen und geht im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der wir, unsere Beschäftigten oder durch uns Beauftragte mit personenbezogenen Daten in Berührung kommen, die von dir stammen oder für dich erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages.

3 Weisungsrecht

(1) Elopay darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen in diesem Vertrag von dir erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Werden wir durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilen wir dir diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen von dir werden durch diesen Vertrag festgelegt und können von dir danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Du bist zu jeder Zeit berechtigt, eine solche Weisung zu erteilen.

Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Bitte richte deine Anfragen an datenschutz@elopage.com.

(3) Du solltest bitte eventuelle Weisungen dokumentieren und speichern- wir werden dieses ebenfalls machen.

Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Sind wir der Ansicht, dass deine Weisung gegen datenschutzrechtliche Bestimmungen verstößt, werden wir dich darauf hinweisen.

Wir sind berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch dich bestätigt oder geändert wird.

Die Durchführung einer offensichtlich rechtswidrigen Weisung dürfen wir ablehnen.

4 Art der verarbeiteten Daten und Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhalten wir Zugriff auf die in Anlage 2 näher spezifizierten personenbezogenen Daten. Diese Daten umfassen keine besonderen Kategorien personenbezogener Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist ebenfalls in Anlage 2 dargestellt.

5 Unsere Schutzmaßnahmen

(1) Wir sind verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Kunden erlangten Informationen nicht ohne Auftrag an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Wir gestalten unseren Verantwortungsbereich und unsere innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Wir treffen alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten von dir (Auftraggebers gem. Art. 32 DS-GVO) insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Trennungsgebot

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt uns vorbehalten, wobei sichergestellt wird, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Unser Ansprechpartner für den Datenschutz ist Özkan Akkilic, datenschutz@elopage.com. Wir veröffentlicht die Kontaktdaten unseres Datenschutzbeauftragten auf unserer Internetseite.

(4) Den bei uns beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Wir werden alle Personen, die von uns mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen werden so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und uns bestehen bleiben. Dir sind die Verpflichtungen auf Anfrage nachzuweisen.

6 Unsere Informationspflichten

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch uns, bei uns im Rahmen des Auftrags beschäftigten Personen oder durch Dritte werden wir dich unverzüglich in Schrift- oder Textform informieren. Dasselbe gilt für Prüfungen von elopay durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von elopay ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Wir treffen unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informieren dich hierüber.

(3) Wir sind darüber hinaus verpflichtet, dir jederzeit Auskünfte zu erteilen, soweit deine Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 werden wir dich zeitnah unterrichten.

(5) Wir führen ein Verzeichnis zu allen Kategorien von im Auftrag von dir durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält.

7 Kontrollrechte des Kunden

(1) Wir verpflichtet uns, dir auf dessen schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen erforderlich sind.

(2) Auf Wunsch stellen wir dir ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(3) Auf Anfrage weisen wir dir die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf nach.

8 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 4 genannten Subunternehmer durchgeführt.

Wir sind im Rahmen unserer vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Wir setzen dich davon in Kenntnis.

(2) Wir wählen jeden Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit aus. Wir achten darauf, dass wir unsere Verpflichtungen dir gegenüber auch (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen können. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat elopay sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Elopay wird dem Kunden auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(3) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn wir Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die wir für dich erbringen und Bewachungsdienste.

9 Anfragen und Rechte Betroffener

(1) Wir unterstützen dich nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung deiner Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber uns geltend, so reagiert wir nicht selbstständig, sondern verweisen den Betroffenen an dich und wartet dessen Weisungen ab.

10 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, bist im Innenverhältnis zu uns alleine du gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

11 Beendigung des Hauptvertrags

(1) Wir werden dir nach Beendigung des Hauptvertrags oder jederzeit auf deine Anforderung alle Daten zurückgeben oder – auf deinen Wunsch hin, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen durch uns oder unsere Subunternehmer. Wir haben hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Wir verpflichten uns, auch über das Ende des Hauptvertrags hinaus die im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie wir über personenbezogene Daten verfügen, die uns von dir zugeleitet wurden oder die wir für diesen erhoben haben.

12 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen Textform. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(3) Diese Vereinbarung unterliegt deutschem Recht unter Ausschluss des in Deutschland geltenden UN-Kaufrechts. Ausschließlicher Gerichtsstand ist Berlin.

Anlagen

Anlage 1 – Leistungsbeschreibung

Anlage 2 - Beschreibung der Datenkategorien/ Beschreibung der Betroffenen/Betroffenengruppen

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 4 – Genehmigte Subunternehmer

Elektronisch signiert am: 31.05.2019

Auftragsverarbeiter: elopay GmbH, Özkan Akkilic (Geschäftsführer)

Verantwortlicher: Martina Baehr, Projektmanagement plus Martina Baehr

Anlage 1: Beschreibung der angebotenen Leistungen

- PayPal

  Verbinde dein PayPal-Konto mit deinen elopages.

- Individuelle Bezahlseiten

  Bezahlseiten, die genau zu deinem Business passen.

- Unbegrenzte Produkte, Bandbreite, Speicher & Kunden

  Baue dein Online-Business ohne Grenzen.

- Produktseiten

  Automatische Produktseiten.

- Visa & Mastercard

  Biete deinem Kunden an, per Visa & Mastercard zu zahlen.

- Online-Kurse

  Online-Kurse, Video-Kurse, Mitgliederbereiche und mehr!

- Videos

  Uploade und streame deine Kurs-Videos direkt über elopage

- Kaufen-Buttons & Widgets

  Integriere deine elopage direkt in deiner Webseite.

- Sofortüberweisung

  Zahlungen per Sofortüberweisung freischalten.

- Shopseite

  Mit deinem ersten Produkt wird automatisch ein Shop für dich erstellt den du optional nutzen kannst, wenn du nicht direkt per Landingpage auf deine Bezahlseite verlinken möchtest

- Kundenverwaltung

  Verwalte und behalte den Überblick über deine Kunden.

- Digitale Produkte

  Verkaufe digitale Produkte oder Dienstleistungen.

- Vorkasse

  Für bestimmte Produkte die Zahlungsart Vorkasse anbieten

- Verschlüsselte Datenübermittlung

  Mehr Sicherheit durch verschlüsselte Daten und Seiten.

- Kauf auf Rechnung

  Mehr Zahlungskomfort für deine Kunden.

- Optimiert für Smartphones & Tablets

  Ohne Probleme über mobile Endgeräte verkaufen mit dem responsive Design.

- e-Tickets

  Verkaufe Tickets für offline- oder Online-Events wie z.B. Webinare.

- Betrugsschutz in Echzeit

  Überprüfung aller Zahlungsdaten in Echtzeit.

- Netto- oder Bruttopreis

  Netto- oder Bruttopreise pro Produkt einstellen

- Zahlungspläne

  Lege einen oder mehrere Zahlungspläne pro Produkt an.

- Download-Produkte

  Verkaufe Download-Produkte wie eBooks oder Software

- Gutschein als Produkt erstellen

  Erstelle Gutscheine als Produkt in nur wenigen Schritten.
- Vorkonfigurierte AGB & Impressum

  Rechtssicheres Impressum und AGB für dein Business.
- Monatlicher Bericht

  Vereinfache deine Buchhaltung mit monatlichen Kontoberichten.
- Automatische Rechnungserstellung

  Versende automatisch Rechnungen bei jedem Verkauf
- Automatische Steuerberechnung

  Sorgenfrei durch den Steuerdschungel.
- Affiliate-Programme

  Erstelle dein eigenes Affiliate-Programm.
- Joint-Venture-Beteiligungen

  Beteilige Partner prozentual an deinen Verkäufen!
- Rechnungserstellung durch Publisher

  Publisher schreiben Rechnungen in deinem Namen.
- Gutscheincodes

  Gutscheincodes oder Rabattcodes sind in wenigen Sekunden in unterschiedlichen Varianten und für verschiedene Anwendungen erstellt.
- Parallel-Tracking

  Leite Affiliate-Traffic auf eine beliebige Landingpage weiter, um deine Conversions zu verbessern.
- Google Analytics

  Nutze Google Analytics für deine elopage Bezahlseite.
- Facebook Pixel

  Optimiere deine Facebook-Kampagnen mit der Pixel-Integration und optimiere deine Ausgaben.
- Upsell & Bundles

  Erhöhe deine Verkäufe durch Upsell und Bundles.
- Sales-Funnel

  Erstelle deine eigenen Sales-Funnel und erhöhe deine Verkäufe.
- Individuelles CSS

  Individualisiere deine Seiten durch eigenes CSS.
- Kurs-Einblick

  Gib deinen Kunden eine Vorschau auf bestimmte Lektionen.
- Zusatzgebühren

  Berechne zusätzliche Lieferkosten oder Gebühren.
- Individuelle Steuersätze

  Lege genau die Steuersätze an, die du brauchst.
- Kunden-Export

  Exportiere deine Kunden-Daten mit nur einem Klick!
- Kampagnen

  Mit den Kampagnen-IDs bietet elopage eine einfache und effektive Tracking-Methode per URL-Parameter.
- URL-Parameter übergeben

  Per URL-Parameter Informationen zum Kauf an eine beliebige URL weitergeben.
- Steuerberichte

  Generiere Berichte über die abzuführenden Steuern für deinen Steuerberater.

- Buchhaltungs-Export

  Buchhaltung leicht gemacht.

- API & Plugin

  Andere Systeme verkaufen mit API und Plugin.

- E-Mail-Rechnungen

  Versende E-Mail-Rechnungen mit besonderen Angeboten.

- Kurs E-Mails

  Verschicke automatisch E-Mails bei bestimmen Aktionen im Kurs.

- Corporate Identity

  Gestalte deine elopages in deinem Corporate Design.

- Auszahlungen

  Regelmäßige Auszahlungen ohne Gebühren.

- Mediathek

  Alle deine Dateien an einem Ort.

- Quiz

  Erstelle Quizze für deine Online-Kurse.

- Drip-In

  Schalte Lektionen automatisch frei.

- Webhooks

  Webhooks können dafür verwendet werden, um deinem System bzw. Server Informationen in Echzeit über Zahlungseingänge und Aktualisierungen zu senden.

- Zusatzfelder

  Ergänze deine Bezahlseiten durch Zusatzfelder und Opt-Ins.

- Tracking-Codes

  Du schaltest Anzeigen? Du möchtest deinen ROI messen? Dann nutze Tracking-Codes, um dein Marketing zu optimieren.

- Statistiken und Analysen

  Erhalte durch Analysen Überblick über deinen Erfolg

- Individuelle Seiten

  Nutze individuelle Seiten für dein Online-Business.

- Kurskommentare

  Erlaube Kommentare in deinem Online-Kurs

- Unbegrenzte Kurs-Lektionen

  Erstelle Online-Kurse ohne Limits

- Landingpages

  Nutze eigene Landingpages für deine Kampagnen

Anlage 2 Datenkategorien und der gespeicherten Daten

1 Art der Daten (Datenkategorie):

- Personenstammdaten (Name, Vorname, Adresse)
- Kommunikationsdaten (E-Mail-Adresse, Telefonnummer)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie (z.B. Login, Produktnutzung, gekaufte Produkte)
- Vertragsabrechnungs- und Zahlungsdaten (z.B. Zahlungsmethode, Zahlungsstatus, Rechnungen)
- Planungs- und Steuerungsdaten (z.B. Besucherquellen, Anzahl Aufrufe, besuchte Seiten, Klicks)
- Technische Daten (z.B. IP-Adresse, Gerät, Browser, Standort, Mac-Adresse)
- Inhaltsdaten (z.B. Videos, Bilder, Texte, Audios, Dateien, Kurskommentare, Antworten auf Quizfragen)

2 Zweck der Datenverarbeitung

Vertragsabwicklung zur Erfüllung der bei uns durch den Kunden gebuchten Leistungen – siehe Beschreibung unter Anlage 1

3 Betroffene Personen

- Webseitenbesucher
- Kunden
- Partner (Publisher, Teammitglieder, Joint-Venture-Partner)

Anlage 3: Technische und organisatorische Maßnahmen

1 Zutrittskontrolle

Darunter sind Maßnahmen zu verstehen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Die Büroräume der elopay befinden sich in einem Gebäude mit Büros und Wohneinheiten in Berlin. In dem Bürogebäude befinden sich Büros von ca. 10 Unternehmen. Der Eingang des Gebäudekomplexes ist mit einer Zutrittstür gesichert, die zwischen 20 Uhr und 7 Uhr verschlossen ist. Das Schlüsselmanagement für die Zutrittstür zum Gebäudekomplex liegt beim Vermieter. Die vom Vermieter ausgegebenen Schlüssel sind dem jeweiligen Mieter zugeordnet. Die Verwaltung der einzelnen Schlüssel der elopay für die Zutrittstür obliegt der elopay selbst.

Die Tür zu den Geschäftsräumen und Fenster der elopay sind Alarmgesichert mit Anbindung an die Notrufleitstelle.

Diesbezüglich gibt es einen Prozess für die Ausgabe von Schlüsseln auf Basis eines 4-Augen-Prinzips. Die Ausgabe von Schlüsseln wird protokolliert. Mitarbeiter sind verpflichtet, einen Schlüsselverlust unverzüglich zu melden. Im Falle eines Verlusts erfolgt ein sofortiger Austausch des Schließsystems.

Ferner gibt es einen Prozess bei einem Ausscheiden eines Mitarbeiters, der insbesondere auch die Rückgabe von Schlüsseln und sonstigem Eigentum der elopay durch den ausscheidenden Mitarbeiter beinhaltet.

Die Büroräume der elopay sind durch eine Alarmanlage mit Videoaufzeichnung gesichert. Die Alarmanlage in den Büroräumen der elopay wird durch den jeweils letzten Mitarbeiter bei Verlassen der Büroräume aktiviert. Zudem gibt es eine automatische Aktivierung der Alarmanlage um 21 Uhr, die verhindern soll, dass eine Aktivierung der Alarmanlage durch einen Mitarbeiter vergessen wird. Aktivierung und Deaktivierung der Alarmanlage erfolgen durch einen Token, den Mitarbeiter erhalten. Auch hierfür gilt der Schlüsselausgabe-Prozess. Die Token sind mit einer Nummer versehen, die dem jeweiligen Mitarbeiter intern zugeordnet werden kann. In der Alarmanlage werden Aktivierungen und Deaktivierungen auf Basis der Token-Nummer protokolliert.

Die Büroräume der elopay befinden sich im 5. Stockwerk des Bürogebäudes. Die Fenster in den Büroräumen der elopay sind für Dritte nicht zugänglich.

Daten der elopay, die im Auftrag verarbeitet werden, werden ausschließlich im AWS-Rechenzentrum von Amazon in Frankfurt gespeichert. Dort sind folgende Maßnahmen zur Zutrittskontrolle getroffen:

- Das AWS-Rechenzentrum und die dort verwendeten Systeme sind in unscheinbaren Gebäuden untergebracht, die von außen nicht sofort als Rechenzentrum zu erkennen sind.
- Das Rechenzentrum selbst ist durch physische Sicherheitsmaßnahmen geschützt, um den unberechtigten Zutritt sowohl weiträumig (z. B. Zaun, Wände) als auch in den Gebäuden selbst zu verhindern.
- Der Zutritt zum Rechenzentrum wird durch elektronische Zugangskontrollen verwaltet und durch Alarmanlagen gesichert, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird.
- Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiter- oder Lieferantendatensatz deaktiviert wurde.
- Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet.
- Zutritt zu sensiblen Bereichen wird durch Videoüberwachung überwacht.
- Ausgebildete Sicherheitskräfte bewachen das AWS-Rechenzentrum und die unmittelbare Umgebung davon 24 Stunden am Tag, 7 Tage die Woche.

2 Zugangskontrolle

Darunter sind Maßnahmen zu verstehen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Die Büroräume der elopay befinden sich im 5. Stock. Die Fenster sind durch gegenüberliegende Büros auf gleich Höhe einsehbar. Die Bildschirme der Mitarbeiter sind jedoch stets so ausgerichtet, dass eine Einsichtnahme von außen nicht erfolgen kann.

An jedem IT-System, das bei der elopay im Einsatz ist, muss eine vorherige Authentifizierung erfolgen. Dies erfolgt auf Basis eines Benutzernamens und eines Passworts.

Eine Berechtigung zur Nutzung eines IT-Systems oder einer Applikation wird bei der elopay nach dem 4-Augen-Prinzip erteilt. Eine Berechtigung muss daher zwingend vom jeweiligen Vorgesetzten für einen Mitarbeiter bei der IT-Administration beantragt werden. Der Vorgesetzte ist verpflichtet, hierbei nur die Berechtigungen zu beantragen, die für den jeweiligen Mitarbeiter unbedingt erforderlich sind, damit dieser die ihm zugewiesenen Aufgaben erfüllen kann. Berechtigungen sind dabei auf das Mindestmaß zu beschränken.

Erteilte Berechtigungen (und der Entzug) werden von der IT-Administration protokolliert. Die IT-Administration prüft quartalsweise in Absprache mit den Vorgesetzten, ob die erteilten Berechtigungen noch erforderlich sind. Vorgesetzte sind darüber hinaus verpflichtet, im Falle von Aufgabenwechsel von Mitarbeitern eine entsprechende Korrektur von Berechtigungen bei der IT-Administration zu beantragen.

Im Falle des Ausscheidens von Mitarbeiter informieren die Personalverantwortlichen die IT-Administration unverzüglich über anstehende Veränderungen, damit die IT-Administration entsprechende Berechtigungen entziehen kann. Der Entzug von Berechtigungen muss binnen 24 Stunden nach Ausscheiden eines Mitarbeiters durchgeführt worden sein.

Werden Initialpasswörter vergeben, ist bei der elopay stets vorgesehen, dass das Initialpasswort bei der ersten Anmeldung geändert wird. Dies wird technisch erzwungen.

Bei der elopay gibt es Richtlinien zur Passwortverwendung, die ebenfalls grundsätzlich technisch erzwungen werden. Die Mindestpasswortlänge beträgt 10 Zeichen. Passwörter sind komplex zu wählen. Dies beinhaltet die Verwendung von Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern, wobei mindestens 3 von 4 dieser Merkmale erfüllt sein müssen.

Ein Passwortwechsel ist spätestens nach 90 Tagen zwingend. Es ist sichergestellt, dass die letzten 10 verwendeten Passwörter eines Nutzers nicht von diesem wiederverwendet werden können.

Ein Zugriff auf die externen IT-Systeme findet ausschließlich über verschlüsselte Verbindungen statt. Die dabei verwendeten Verschlüsselungsalgorithmen und Schlüssellängen entsprechen dem Stand der Technik.

Alle IT-Systeme, mit denen Daten im Auftrag verarbeitet werden, sind mit Antivirus-Software ausgestattet.

Für das AWS-Rechenzentrum gilt, dass auch dort alle Berechtigungen nach dem Prinzip der Minimalberechtigung erteilt und Berechtigungen regelmäßig überprüft werden. Die Vergabe und der Entzug von Berechtigungen wird protokolliert. Die Verwendung von Passwörtern ist ebenfalls geregelt und sieht die Verwendung von komplexen Passwörtern, einen Passwortwechsel nach spätestens 90 Tagen sowie eine Passworthistorie vor.

3 Zugriffskontrolle

Darunter sind Maßnahmen zu verstehen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Für die Erteilung von Benutzerrechten gilt bei der elopay ein Berechtigungskonzept. Dies sieht vor, dass Berechtigungen ausschließlich auf Basis des 4-Augenprinzips und nach dem Minimalprinzip vergeben werden. Dies beinhaltet, dass jeder Mitarbeiter nur die Berechtigungen erhält, die er unmittelbar benötigt, um seine Aufgaben im Unternehmen erfüllen zu können.

Das Berechtigungskonzept ist rollenbasiert. Jedem Mitarbeiter wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende Berechtigungen müssen begründet sein.

Die Vergabe und der Entzug von Berechtigungen wird protokolliert. Eine quartalsweise Überprüfung erfolgt durch die IT-Administration in Zusammenarbeit mit den jeweiligen Vorgesetzten der Mitarbeiter.

4 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Dadurch, dass Berechtigungen nach dem Minimalprinzip vergeben werden, ist gewährleistet, dass der Kreis der Personen, die Zugang zu Daten hat, die im Auftrag verarbeitet werden, beschränkt ist. Ein Kopieren von Daten auf externe Datenträger ist systemseitig unterbunden.

Ein Export von Daten wird auf Applikationsebene protokolliert und für einen Zeitraum von 12 Monaten unter Angabe der jeweiligen Benutzerkennung gespeichert.

Jeder Zugriff auf und der Abruf von Daten der Applikation erfolgt verschlüsselt (TLS).

Sofern Daten im Einzelfall auf Anfrage des Auftraggebers an diesen durch die elopay übergeben werden soll, werden die Parteien im Vorwege eine Verschlüsselungsmethode bzw. einen Weg der sicheren Übertragung vereinbaren.

5 Eingabekontrolle

Darunter sind Maßnahmen zu verstehen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Jede Eingabe von Daten, die im Auftrag des Auftraggebers von der elopay verarbeitet werden, wird systemseitig unter Zuordnung der jeweiligen Benutzerkennung protokolliert. Gleiches gilt für die Änderung und Löschung von Daten. Im Falle einer Änderung von Daten ist aus der Protokollierung erkenntlich, welche Änderungen vorgenommen wurden.

Die Protokolle werden für die Dauer der Vertragslaufzeit von der elopay gespeichert. Eine vorherige Löschung kann zwischen den Parteien vereinbart werden.

Durch die Protokollierung ist jederzeit nachvollziehbar, welche Benutzer Daten eingegeben, geändert oder gelöscht hat.

6 Auftragskontrolle

Darunter sind Maßnahmen zu verstehen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Der Schutz personenbezogener Daten und auch der Schutz von Betriebs- und Geschäftsgeheimnissen hat bei der elopay eine hohe Priorität. Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet.

Es gibt einen betrieblichen Datenschutzbeauftragten, der auch die regelmäßige Schulung der Mitarbeiter plant und durchführt. Alle Mitarbeiter erhalten mindestens eine jährliche Datenschutzschulung bzw. eine „Auffrischung“.

Mitarbeiter, die an der Erbringung von Leistungen für den Auftraggeber beteiligt sind, sind im Hinblick auf die Verarbeitung der Daten instruiert. Sofern der Auftraggeber ergänzende Weisungen erteilt, wird die elopay alle betroffenen Mitarbeiter unverzüglich über die jeweilige Weisung informieren und Handlungsanweisungen zur Umsetzung geben.

Die Datenschutzvorkehrungen der elopay beinhalten auch eine regelmäßige Überprüfung und Bewertung der getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit. Hierzu gehört auch ein Verbesserungs- und Vorschlagswesen, an dem sich Mitarbeiter beteiligen können. Die elopay gewährleistet so eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten.

7 Verfügbarkeitskontrolle

Darunter sind Maßnahmen zu verstehen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Alle Daten, die für den Auftraggeber verarbeitet werden, befinden sich im AWS-Rechenzentrum. Elopay hat Maßnahmen getroffen, die eine Sicherung der Daten und Wiederherstellung von Daten mit redundanten System gewährleistet. Es gibt ein Datensicherungs- und Wiederherstellungskonzept, das regelmäßig getestet wird.

Im AWS-Rechenzentrum sind umfangreiche Maßnahmen zur Gewährleistung der Verfügbarkeit getroffen:

Im Rechenzentrum ist eine automatische Branderkennung und -bekämpfung installiert. Das Branderkennungssystem setzt Rauchsensoren in der gesamten Umgebung der Rechenzentren, in mechanischen und elektrischen Bereichen der Infrastruktur, Kühlräumen und sowie in den Räumen, in denen die Generatoren untergebracht sind, ein.

Alle Stromversorgungssysteme sind redundant. Eine unterbrechungsfreie Stromversorgung (USV) sorgt im Fall eines Stromausfalls dafür, dass kritische Bereiche der Anlage weiterhin mit Strom versorgt werden. Das Rechenzentrum verfügt darüber hinaus über Generatoren, die die gesamte Anlage mit Notstrom versorgen können.

Das Rechenzentrum verfügt über eine Klimatisierung und Temperaturkontrolle.

Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.

8 Trennungsgebot

Darunter sind Maßnahmen zu verstehen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die IT-Systeme, auf denen Daten im Auftrag verarbeitet werden, sind mandantenfähig. Es ist sichergestellt, dass Daten getrennt voneinander verarbeitet werden.

Anlage 4 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne der Nr. 8:

ActiveCampaign, Inc.

1 N Dearborn, 5th floor
Chicago, Illinois 60602
United States

Funktion:

- Newsletter rund um die Nutzung von elopage an meine Partner (Publisher, Teammitglieder)

Amazon Web Services, Inc.

410 Terry Avenue North
Seattle WA 98109
United States

Funktion:

- Betrieb und Verwaltung der Webseite und Plattform elopage.com

Atlassian Pty Ltd
c/o Atlassian, Inc.
1098 Harrison Street
San Francisco, CA 94103

United States

Funktion:
- Bearbeitung von Störungsmeldungen und Supportanfragen

Google LLC
Unter den Linden 14
10117 Berlin
Deutschland

Funktion:

- Speicherung von Dateien und Versand von Mails im Rahmen der Bearbeitung von Supportanfragen

The Rocket Science Group, LLC

675 Ponce de Leon Ave NE
Suite 5000
Atlanta, GA 30308
United States

Funktion:

- Versand automatisierter Mails rund um das Vertragsverhältnis

Zendesk, Inc.

Rheinsberger Str. 73
10115 Berlin
Deutschland

Funktion:

- Kommunikation mit Kunden und Partnern per Mail / Chat
- Nutzung des Hilfecenters

Stand: 01.07.2018