Datenschutzvereinbarung

Zweck dieses Anhangs ist es, die Bedingungen festzulegen, unter denen sich der Provider in seiner Eigenschaft als Auftragsverarbeiter im Sinne der nachstehenden Definition verpflichtet, die Verarbeitung personenbezogener Daten im Auftrag des Kunden im Rahmen des Vertrags zu verarbeiten.

Der Provider ist befugt, im Auftrag des Kunden die für die Erbringung der Dienstleistung erforderlichen personenbezogenen Daten zu verarbeiten. Die Art der mit den personenbezogenen Daten durchgeführten Verarbeitungsvorgänge umfasst deren Speicherung und die kontrollierte Bereitstellung der personenbezogenen Daten gegenüber dem Kunden. Die Zwecke der Verarbeitungen, die Liste der verarbeiteten personenbezogenen Daten und die Kategorien der betroffenen Personen sind im Folgenden definiert.

1. Definitionen

Für die Zwecke dieses Anhangs und ungeachtet anderer Definitionen im Vertrag haben die in diesem Anhang in Großbuchstaben geschriebenen Begriffe, ob im Singular oder Plural, die folgende Bedeutung:

Datenschutzgesetze: sind die in der Europäischen Union, dem Europäischen Wirtschaftsraum und ihren Mitgliedstaaten geltenden Gesetze und Vorschriften über die Verarbeitung personenbezogener Daten, insbesondere das Bundesdatenschutzgesetz vom 30. Juni 2017 (BDSG) und die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (die "Datenschutzgrundverordnung" oder "DSGVO").

Betroffene Person: jede identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten Gegenstand der Verarbeitung sind. Als "identifizierbare natürliche Person" wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer oder zu einer Online-Kennung.

Verantwortlicher: jede Stelle, die die Zwecke und Mittel der Datenverarbeitung bestimmt. Für die Zwecke des Vertrags handelt der Kunde gegenüber dem Provider als der für die Verarbeitung Verantwortliche.

Auftragsverarbeiter: bezeichnet eine Stelle, die personenbezogene Daten im Auftrag, auf Anweisung und unter der Autorität des für die Verarbeitung Verantwortlichen verarbeitet. Für die Zwecke des Vertrages handelt der Provider als Auftragsverarbeiter.

Verarbeitung: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten oder einer Reihe personenbezogener Daten wie das Erheben, das Speichern, die Organisation, die Strukturierung, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Übermittlung durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, den Abgleich oder die Verknüpfung sowie die Einschränkung, Löschung oder Vernichtung.

Verletzung des Schutzes personenbezogener Daten: bezeichnet eine Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Weitergabe oder zum Zugriff auf übermittelte, gespeicherte und/oder anderweitig verarbeitete personenbezogene Daten führt.

2. Zwecke der Verarbeitung

Der Provider ist befugt, im Namen des Kunden die personenbezogenen Daten zu verarbeiten, die zur Erbringung der im Vertrag nebst Anlagen beschriebenen Services erforderlich sind.

Die personenbezogenen Daten sind Gegenstand der folgenden grundlegenden Verarbeitungstätigkeiten:

Organisation; Speicherung; Hosting; Wartung; Beratung, Verbreitung, Aufzeichnung, Registrierung und Änderung durch den Kunden.

Der Zweck der Verarbeitung ist die Ausführung der im Vertrag beschriebenen Services.

Die verarbeiteten personenbezogenen Daten beziehen sich auf die folgenden Kategorien von Daten:

- Identifizierungsdaten: Vorname, Nachname, Telefonnummer, E-Mail-Adresse, Foto des Benutzerprofils.
- Berufliche Daten: Position, Organigramm, etc.
- Verbindungsdaten: Protokolle.
- Internetdaten: Cookies, IP.

Die Kategorien der betroffenen Personen sind die Nutzer der Services und autorisierte Personen, deren Identifizierung notwendig ist, um die Bereitstellung der Services zu gewährleisten.

Die personenbezogenen Daten werden vom Kunden erfasst, der sie auf der Plattform, die die Services bereitstellt, eingibt oder importiert. Der Kunde importiert auch die für die Verarbeitung erforderlichen Dokumente, die personenbezogene Daten enthalten können, und legt die Berechtigungsstufen fest, die den Nutzern der Services gewährt werden sollen.

3. Allgemeine Verpflichtungen

Der Provider verpflichtet sich:

- die personenbezogenen Daten nur für den/die Zweck(e) zu verarbeiten, der/die mit den im Vertrag beschriebenen Services in Zusammenhang steht/stehen.
- die personenbezogenen Daten gemäß den dokumentierten Anweisungen des Auftraggebers zu verarbeiten.
  Wenn der Provider der Ansicht ist, dass eine Anweisung einen Verstoß gegen die DSGVO oder eine andere Bestimmung des EU-Rechts oder des Rechts eines Mitgliedstaats in Bezug auf den Datenschutz darstellt, informiert er den Kunden unverzüglich. Wenn der Provider nach dem EU-Recht oder dem Recht des Mitgliedstaats, dem er unterliegt, verpflichtet ist, personenbezogene Daten an ein Drittland oder eine internationale Organisation zu übermitteln, informiert er den Kunden vor der Verarbeitung über diese rechtliche Verpflichtung, es sei denn, das betreffende Gesetz verbietet eine solche Information aus wichtigen Gründen des öffentlichen Interesses.
- die Vertraulichkeit der im Rahmen dieses Vertrages verarbeiteten personenbezogenen Daten zu gewährleisten.
- sicherzustellen, dass die Personen, die im Rahmen dieses Vertrages zur Verarbeitung personenbezogener Daten befugt sind:
  - zur Vertraulichkeit verpflichtet sind oder einer entsprechenden gesetzlichen Verpflichtung zur Vertraulichkeit unterliegen;
  - die erforderlichen Schulungen zum Schutz personenbezogener Daten erhalten.

bei seinen Tools, Produkten, Anwendungen oder Services die Grundsätze von „Privacy by design“ und „Privacy by default“ zu berücksichtigen.

4. Weisungen des Kunden

Die Services sind ein Standardservice, der von allen Kunden auf die gleiche Weise genutzt werden kann.

Am Tag der Unterzeichnung stellt der Vertrag die schriftliche Weisung des Kunden an den Provider dar, im Rahmen der Bedingungen und Grenzen des Vertrages personenbezogene Daten zu verarbeiten.

5. Unterauftragsverarbeiter

Der Provider ist berechtigt, die Dienste der folgenden Unternehmen (im Folgenden "**Unterauftragsverarbeiter**" genannt) in Anspruch zu nehmen:

OVH GROUPE SA, 2 rue Kellermann, 59100 Roubaix	Frankreich	das Hosting der Server, auf denen die personenbezogenen Daten gespeichert sind, und ihre Anbindung an das Internet

Der Provider kann einen oder mehrere Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten beauftragen. In diesem Fall informiert der Provider den Kunden im Voraus schriftlich über alle geplanten Änderungen in Bezug auf die Hinzufügung oder den Austausch anderer Unterauftragsverarbeiter. Der für die Verarbeitung Verantwortliche kann binnen einer Frist von zehn (10) Tagen ab dem Datum des Erhalts der Mitteilung über die geplante Änderung beim Einsatz von Unterauftragsverarbeitern Einspruch erheben. Diese Unterauftragsverarbeitung darf nur durchgeführt werden, wenn der Auftraggeber innerhalb der oben genannten Frist keine Einwände erhoben hat. Der Kunde wird die Genehmigung zur Einbindung weiterer Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter nicht ohne wichtigen Grund verweigern.

Der Provider wird mit Unterauftragsverarbeitern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen dieses Vertrages im Wesentlichen entsprechen. Der Provider ist dafür verantwortlich, dass der Unterauftragsverarbeiter dieselben ausreichenden Garantien hinsichtlich der Umsetzung geeigneter technischer und organisatorischer Maßnahmen bietet, damit die Verarbeitung den Anforderungen der DSGVO entspricht. Kommt der Unterauftragsverarbeiter seinen Verpflichtungen in Bezug auf den Schutz personenbezogener Daten nicht nach, bleibt der Provider gegenüber dem Kunden in vollem Umfang für die Erfüllung seiner Verpflichtungen durch den Unterauftragsverarbeiter verantwortlich.

6. Informationsrechte der betroffenen Personen

Der Kunde ist dafür verantwortlich, die von der Verarbeitung betroffenen Personen (Nutzer des Dienstes) zum Zeitpunkt der Erhebung der personenbezogenen Daten zu informieren.

7. Ausübung der Rechte der betroffenen Personen

Der Provider muss im Namen und im Auftrag des Kunden innerhalb der in der DSGVO vorgesehenen Fristen auf Anträge der betroffenen Personen zur Ausübung ihrer Rechte in Bezug auf Daten, die unter die in diesem Vertrag vorgesehene Verarbeitung fallen, reagieren.

8. Meldung von Datenschutzverletzungen

Der Provider benachrichtigt den Kunden über jede Verletzung des Schutzes personenbezogener Daten spätestens achtundvierzig (48) Stunden, nachdem er davon Kenntnis erlangt hat, und zwar per E-Mail an den Datenschutzbeauftragten des Kunden oder seinen bevollmächtigten Vertreter. Dieser Benachrichtigung sind alle zweckdienlichen Unterlagen beizufügen, die es dem Kunden ermöglichen, diese Verletzung gegebenenfalls bei der zuständigen Aufsichtsbehörde zu melden.

Die Mitteilung muss mindestens folgende Angaben enthalten

- Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, einschließlich, wenn möglich, der Kategorien und der ungefähren Anzahl der von der Verletzung betroffenen Personen sowie der Kategorien und der ungefähren Anzahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Kontaktstelle, bei der zusätzliche Informationen eingeholt werden können;
- die voraussichtlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- die vom Provider ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, gegebenenfalls einschließlich der Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen.

Wenn und soweit es nicht möglich ist, alle diese Informationen auf einmal zu übermitteln, können die Informationen ohne unangemessene Verzögerung schrittweise bereitgestellt werden.
Die Benachrichtigung der betroffenen Person erfolgt durch den Kunden, der allein in der Lage ist, das Risiko für die Rechte und Freiheiten einer natürlichen Person zu beurteilen.

9. Unterstützung des Providers bei der Erfüllung der Verpflichtungen des Kunden

Der Provider unterstützt den Kunden bei der Durchführung von Datenschutzfolgenabschätzungen in Bezug auf den Schutz personenbezogener Daten.

Der Provider unterstützt den Kunden bei der Durchführung der vorherigen Konsultation mit der Aufsichtsbehörde.

10. Sicherheitsmaßnahmen

Der Provider verpflichtet sich, die im SLA und im Vertrag festgelegten Sicherheitsmaßnahmen umzusetzen.

11. Verbleib der persönlichen Daten

Der Provider verpflichtet sich, die im Service Level Agreement (SLA) zu dieser Datenschutzvereinbarung festgelegten technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Daten einzusetzen. Das SLA stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Provider dar.

Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Provider vorbehalten, sofern sichergestellt ist, dass auch nach der Änderung das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Das SLA wird in diesem Fall entsprechend durch den Provider geändert und wird in seiner geänderten Fassung Bestandteil dieser Vereinbarung, sofern der Kunde nicht innerhalb angemessener Frist der Änderung aus berechtigtem Anlass widerspricht.

12. Verzeichnis der Kategorien von Verarbeitungstätigkeiten

Der Provider erklärt, dass er ein schriftliches Verzeichnis aller Kategorien von Verarbeitungstätigkeiten führt, die im Auftrag des Kunden durchgeführt werden, einschließlich:

- den Namen und die Kontaktdaten des Auftraggebers, in dessen Namen er handelt, der Unterauftragsverarbeiter und ggf. des Datenschutzbeauftragten;
- die Kategorien der im Auftrag des Auftraggebers durchgeführten Verarbeitungen;
- im ausdrücklichen Fall einer gerichtlichen Anordnung die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des Drittlandes oder der internationalen Organisation und - im Fall der in Artikel 49 Absatz 1 Unterabsatz 2 der

Datenschutz-Grundverordnung genannten Übermittlungen - der Dokumente, die das Vorhandensein angemessener Garantien belegen;

- soweit möglich, eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die unter anderem, soweit zutreffend, folgende Angaben enthalten
    - Pseudonymisierung und Verschlüsselung von personenbezogenen Daten;
    - Mittel zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit von Verarbeitungssystemen und -diensten;
    - Mittel zur rechtzeitigen Wiederherstellung der Verfügbarkeit von und des Zugangs zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls
    - ein Verfahren zur regelmäßigen Prüfung, Analyse und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

13. Dokumentation

Der Provider stellt dem Kunden die Unterlagen zur Verfügung, die erforderlich sind, um die Einhaltung aller seiner Verpflichtungen nachzuweisen und um Audits, einschließlich Inspektionen, durch den Kunden oder einen anderen vom Kunden beauftragten Prüfer zu ermöglichen und zu unterstützen.

14. Datenschutzbeauftragter

Die Kontaktdaten des Datenschutzbeauftragten des Providers lauten: contact-DPO@dilitrust.com