Auftragsverarbeitungsvertrag gemäss Art. 9 des Bundesgesetzes über den Datenschutz vom 25. September 2020

Dieser Auftragsverarbeitungsvertrag (dieser «AVV») gilt zwischen der Eturnity AG («Eturnity») und allen Kundinnen und Kunden der Eturnity mit Sitz in der Schweiz (der «Auftraggeber»). Dieser AVV erweitert das bestehende Vertragsverhältnis zwischen Eturnity und dem Auftraggeber.

1. Art der Datenverarbeitung

Art und Zweck der vorgesehenen Verarbeitung von Daten: Online Erfassung von personenbezogenen Daten über einen Workflow im Internet. Erstellung von PV Konzepten in Form eines PDFs und optionale Weitergabe der Daten an den Auftraggeber bei expliziter Zustimmung.

Art der personenbezogenen Daten: Identifikationsdaten (Name, Adresse), Kontaktdaten (E-Mail-Adresse, Telefonnummer). Es werden keine besonders schützenswerte Personendaten bearbeitet und es besteht kein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen.

Kategorien betroffener Personen: Potenzielle und gewonnene Kundinnen und Kunden von Solar- und Heizungsinstallateuren.

2. Datensicherheit

Eturnity trifft folgende technischen und organisatorischen Massnahmen (TOM) zur Sicherstellung der Datensicherheit:

3. Bekanntgabe von Personendaten ins Ausland

Eturnity bezieht Dienstleistungen von den nachfolgenden Unternehmen im Ausland. Im Rahmen

dieses Dienstleistungsbezugs können Personendaten an folgende Unternehmen respektive in

folgende Länder übermittelt werden:

Unternehmen im Ausland	**Land**	**Angemessener Schutz**
PDFCrowd s.r.o.	Tschechien	Gemäss Art. 8 Abs. 1 DSV
Digital Ocean, LLC	USA	Gemäss Art. 16 Abs. 2 lit. d DSG
Hetzner Online GmbH	Deutschland	Gemäss Art. 8 Abs. 1 DSV
Cloudflare, Inc.	USA	Gemäss Art. 16 Abs. 2 lit. d DSG
Mailgun Technologies, Inc	USA	Gemäss Art. 16 Abs. 2 lit. d DSG
Microsoft Corporation	USA	Gemäss Art. 16 Abs. 2 lit. d DSG

Eturnity nutzt weitere Unterauftragsverarbeiter nur mit Genehmigung des Auftraggebers. Sie gelten ohne Widerspruch innerhalb von 14 Tagen als genehmigt.

Wo ein Unterauftragsverarbeiter eingesetzt wird, hat Eturnity diesem die gleichen Verpflichtungen wie diejenigen aus diesem AVV aufzuerlegen und sich zu vergewissern, dass der Unterauftragsverarbeiter diese Verpflichtungen einhalten kann.

4. Informationspflicht bei der Beschaffung von Personendaten

Der Auftraggeber hat die betroffene Person angemessen über die Beschaffung der Personendaten zu informieren. Sollten zusätzliche Informationen erforderlich sein, die nicht in diesem AVV enthalten sind, wird Eturnity sie dem Auftraggeber zur Verfügung stellen.

5. Datenschutzberater / Auskunftsrecht / Kontakt

Eturnity ist gemäss Art. 10 DSG nicht verpflichtet, einen Datenschutzberater zu ernennen. Der Auftraggeber kann sich aber jederzeit mit datenschutzrechtlichen Anliegen unter folgender Adresse an Eturnity wenden: support@eturnity.com.

An die oben genannte Adresse können schriftliche Anfragen im Rahmen des gesetzlich verankerten Auskunftsrechts gerichtet werden. Eturnity leitet Begehren betroffener Personen oder Behörden unverzüglich dem Auftraggeber weiter, ohne diese selbst zu beantworten. Eturnity unterstützt den Auftraggeber bei Bedarf bei der Einhaltung des Datenschutzrechts (insbesondere zur Erfüllung von Betroffenenrechten und bei Datenschutz-Folgenabschätzungen).

6. Verzeichnis der Bearbeitungstätigkeiten

Eturnity ist gemäss Art. 24 DSV von der Pflicht ausgenommen, ein Verzeichnis über die Bearbeitungstätigkeiten zu führen.

7. Pflichten von Eturnity

7.1 Eturnity verarbeitet die Daten nur für Zwecke und nur auf dokumentierte Weisung des Auftraggebers. Hält Eturnity die Weisung des Auftraggebers für unzulässig, teilt Eturnity dies dem Auftraggeber unverzüglich mit.

7.2 Eturnity meldet dem Auftraggeber ohne Verzug jede Verletzung der Datensicherheit mit allen Informationen.

7.3 Eturnity verpflichtet alle Hilfspersonen und Mitarbeiter zur Geheimhaltung, soweit sie dies nicht schon von Gesetzes wegen sind.

7.6 Nach Beendigung des AVV gibt Eturnity alle Daten dem Auftraggeber zurück und löscht sie im gesetzlich zulässigen Rahmen.

7.7 Eturnity weist die Einhaltung dieses AVV nach und der Auftraggeber kann sie umfassend überprüfen.

8. Schlussbestimmungen

Dieser AVV ist Bestandteil des zwischen Eturnity und dem Auftraggeber existierenden Vertrags und teilt das rechtliche Schicksal mit Letzterem. In Bezug auf den Gerichtsstand und das anwendbare Recht gelten die Bestimmungen des existierenden Vertrags. Sollten zwischen Eturnity und dem Auftraggeber Abreden bestehen, welche diesem AVV widersprechen, gehen diese Abreden vor, sofern sie nicht gegen geltendes, zwingendes Recht verstossen. Eturnity kann diesen AVV jederzeit anpassen. Die Anpassungen werden nach 14 Tagen wirksam, sofern der Auftraggeber nicht innerhalb dieser 14 Tagen Widerspruch einlegt.

Eturnity AG

Anhang 1: TOM

1. Einleitung

1.1. Verantwortlicher

Verantwortlicher gem. Art. 5 lit. j Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) ist Eturnity AG, Reichsgasse 3, 7000 Chur, Switzerland, E-Mail: info@eturnity.com. Gesetzlich vertreten werden wir durch Pol Budmiger, Matthias Wiget, Manuel Alamillo Frias, Kurt Lüscher, Arnold Marty, Vincent Gregoir.

1.2. Datenschutzberater

Unser Datenschutzberater ist über die heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, E-Mail: datenschutz@heydata.eu erreichbar.

1.3. Gegenstand des Dokuments

Dieses Dokument fasst die vom Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 8 Abs. 1 DSG zusammen. Das sind Maßnahmen, mit denen der Verantwortliche personenbezogene Daten schützt.

2. Vertraulichkeit (Art. 3 Abs. 1 Datenschutzverordnung, DSV)

2.1. Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Manuelles Schließsystem (z.B. Schlüssel)
- Schließsystem mit Codesperre
- Schlüsselregelung / Schlüsselbuch
- Festlegung zutrittsberechtigter Personen
- Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus
- Begleitung von Besuchern und Fremdpersonal
- Arbeit im Home Office: Unbefugte haben kein Zutritt zur Wohnstätte der Mitarbeiter

2.2. Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- Authentifikation mit Benutzer und Passwort
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Verschlüsselung von Datenträgern
- Verschlüsselung von Notebooks / Tablets
- Nutzung von 2-Faktor-Authentifizierung
- Schlüsselregelung / Schlüsselbuch
- Allgemeine Anweisung, bei Verlassen des Arbeitsplatzes Desktop manuell zu sperren
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben
- Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk

2.3. Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Anzahl der Administratoren ist so klein wie möglich gehalten

2.4. Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts

- Festlegung von Datenbankrechten

- Versehen der Datensätze mit Zweckattributen/Datenfeldern

3. Integrität (Art. 3 Abs. 2 DSV)

3.1. Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Bereitstellung von Daten über verschlüsselte Verbindungen wie SFTP oder HTTPS
- Härtung der Backendsysteme
- Maschine-Maschine Authentisierung
- Datenträgerverwaltung (Verfahren)
- Datenschutzgerechtes Lösch-/ Zerstörungsverfahren

4. Nachvollziehbarkeit (Art. 3 Abs. 3 DSV)

4.1. Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

- Protokollierung der Eingabe, Änderung und Löschung von Daten

5. Verfügbarkeit (Art. 3 Abs. 2 DSV)

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- Regelmäßige Backups

- Erstellung eines Backup- & Recoverykonzepts

- Kontrolle des Sicherungsvorgangs

- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Hosting (jedenfalls der wichtigsten Daten) mit einem professionellen Hoster
- Datenschutztresor

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

6.1. Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Verwendung der heyData-Plattform zum Datenschutz-Management
- Stellung des Datenschutzberaters durch heyData
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter im Datenschutz
- Führen eines Verzeichnisses über Bearbeitungstätigkeiten (Art. 12 DSG)

6.2. Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 5 lit. h DSG gegenüber dem EDÖB (Art. 24 Abs. 1 DSG)
- Meldeprozess für Datenschutzverletzungen nach Art. 5 lit. h DSG gegenüber betroffenen Personen (Art. 24 Abs. 4 DSG)
- Einbindung des Datenschutzberaters in Sicherheitsvorfälle und Datenpannen
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls

6.3. Datenschutzfreundliche Voreinstellungen (Art. 7 Abs. 3 DSG)

Die folgenden implementierten Maßnahmen tragen den Voraussetzungen der Prinzipien "Privacy by design" und "Privacy by default" Rechnung:

- Schulung der Mitarbeiter im "Privacy by design" und "Privacy by default"
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

6.4. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Schriftliche Weisungen an den Auftragnehmer oder Weisungen in Textform (z.B. durch Auftragsbearbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen
- Bestätigung von Auftragnehmern, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (typischerweise im Auftragsverarbeitungsvertrag)