INNOVANDO
THE **SWISS** BRANDING COMPANY

Betreff:

Datenschutz-Folgenabschätzung (DPIA)
Rechtsgrundlage: Artikel 35 der EU-Verordnung 2016/679 (DSGVO) – Schweizer Bundesgesetz über den Datenschutz (DSG, revidiert 2023)

Einleitung

Diese *Datenschutz-Folgenabschätzung* (DPIA) wird von **Innovando GmbH (operating as Innovando Swiss)** erstellt, um die Auswirkungen der Verarbeitung personenbezogener Daten im Rahmen ihrer operativen, beratenden und digitalen Tätigkeiten zu bewerten und zu dokumentieren. Ziel dieses Dokuments ist es, die Einhaltung der Grundsätze von *Accountability*, *Privacy by Design* und *Privacy by Default* transparent nachzuweisen und sicherzustellen, dass jede Verarbeitung im vollen Einklang mit den Grundrechten und -freiheiten der betroffenen Personen erfolgt.

Die DPIA dient zugleich als Instrument der Governance und Prävention: Sie ermöglicht die frühzeitige Erkennung potenzieller Risiken, deren Bewertung und die Umsetzung geeigneter technischer und organisatorischer Massnahmen.
Innovando GmbH verpflichtet sich, ein hohes Datenschutzniveau zu gewährleisten, das auf Informationssicherheit, Vertraulichkeit, Integrität und einer verantwortungsvollen Datenverwaltung beruht.

1. Verantwortlicher und organisatorischer Kontext

Verantwortlicher für die Datenverarbeitung
Andreas Arno Michael Voigt
Innovando GmbH
Loretto 4, 9108 Gonten (Schweiz)
Tel. +41 71 794 1500
E-Mail: privacy@innovando.swiss

Technischer Leiter und Informationssicherheitsbeauftragter
Sven Holzhuber, seit 2. Mai 2018

Datenschutzbeauftragter (DPO)
Nicht ernannt, da die Ernennung gemäss DSG und DSGVO aufgrund des Umfangs und der Art der Verarbeitung nicht erforderlich ist.

Zweck der Datenverarbeitung
Die Verarbeitung personenbezogener Daten dient der Analyse, dem Marketing, dem CRM, der regelmässigen und ausserordentlichen Wartung von Websites, der Erstellung strategischer Kommunikationsunterlagen für Kundenunternehmen sowie der administrativen Verwaltung geschäftlicher Beziehungen.

Betroffene Personengruppen
Kunden, Interessenten, Lieferanten, Mitarbeitende und Website-Benutzer.

Kategorien personenbezogener Daten
Name, Vorname, Firmenname, Adresse, E-Mail, Vertragsdaten, Rechnungsdaten, Cookies und Navigationsdaten.

2. Externe Auftragsverarbeiter und Infrastruktur

Externe Auftragsverarbeiter

- **Metanet AG**, Anbieter von Cloud- und Hosting-Diensten (Server in der Schweiz, ISO 27001 zertifiziert).
- **BREVO**, Plattform für Newsletter-Verwaltung.
- **Banca Popolare di Sondrio**, Bankdienstleistungen.
- **PayPal**, Plattform für elektronische Zahlungen.
- **BEXIO**, Buchhaltungssoftware.

Zertifizierungen

- Die Rechenzentren der Partnerunternehmen GTT (Interroute) und Equinix sind nach ISO 27001 zertifiziert.
- Innovando GmbH ist mit den Labels *Swiss Digital Services* und *Swiss Label* ausgezeichnet.

Datenstandort
Alle Daten werden **ausschliesslich in der Schweiz** verarbeitet und gespeichert.
Es findet **keine Datenübermittlung** in Länder ausserhalb der EU oder des EWR statt, die nicht dem DSGVO- oder DSG-Standard entsprechen.

3. Beschreibung der Verarbeitungstätigkeiten

Datenerhebung
Daten werden über Online-Formulare, Newsletter, Cookies, Kontaktformulare, analytisches Tracking, Event-Anmeldungen, Interviews und gegebenenfalls manuell erhoben.

Verarbeitungszwecke
Kommunikation mit Kunden und Lieferanten, Analyse des Webverkehrs, Personalisierung von Inhalten, Remarketing-Aktivitäten und kontinuierliche Verbesserung der Dienstleistungen.

Verwendete Systeme und Tools
Google Analytics, Meta Pixel, CRM-Systeme und KI-gestützte Werkzeuge, die mit dem *EU AI Act* konform sind, wie in der *Declaration on the Use of Artificial Intelligence* auf der offiziellen Website dargelegt.

Aufbewahrungsdauer
Daten werden so lange gespeichert, wie dies zur Erfüllung der beauftragten Aufgaben erforderlich ist, zuzüglich eines operativen Jahres.
Daten von Interessenten werden nach einem Jahr automatisch gelöscht.

4. Sicherheitsmassnahmen und Risikominderung

Die Datensicherheit bei Innovando GmbH basiert auf einer mehrschichtigen Strategie, die den Prinzipien der *Defense in Depth* und *Resilience by Design* folgt.
Jede Systemkomponente ist darauf ausgelegt, den operativen Betrieb auch bei Hardwareausfällen, menschlichen Fehlern oder externen Störungen aufrechtzuerhalten.

Backup-System und 3–2–1-Regel

Innovando wendet konsequent die international anerkannte **3–2–1-Backup-Regel** an:

- **3 Gesamtkopien der Daten** (1 primäre und 2 Sicherungskopien);
- **2 verschiedene Speichermedien**, um das Risiko eines gleichzeitigen Ausfalls zu minimieren;
- **1 Kopie ausserhalb des Standorts**, physisch getrennt von der Produktionsumgebung.

In der Praxis werden die Unternehmensdaten täglich auf einem **primären NAS-System mit RAID-5-Konfiguration** und auf einem **sekundären NAS**, ebenfalls mit RAID 5, in einer separaten physischen Einheit gespiegelt.
Beide Backups sind verschlüsselt und unterliegen regelmässigen Integritätstests.
Diese Architektur stellt sicher, dass selbst im Falle von Hardware-Schäden, physischen Vorfällen oder Naturkatastrophen ein Datenverlust **praktisch ausgeschlossen** ist.

Verschlüsselung und Datenintegrität

Alle Backups werden mit dem Verschlüsselungsstandard **AES-256** gesichert. Die Schlüssel werden in isolierten Umgebungen gespeichert und sind nur für autorisiertes technisches Personal zugänglich.
Datenintegrität wird laufend durch Hash-Prüfungen und automatisierte Kontrollen gewährleistet, um unbemerkte Datenbeschädigungen zu verhindern.

Firewalls, Segmentierung und Aktualisierungen

Das Unternehmensnetzwerk ist durch **dedizierte Hardware-Firewalls** geschützt, die den Datenverkehr segmentieren und unautorisierte Verbindungen blockieren.
Server werden regelmässig aktualisiert, Sicherheits-Patches innerhalb von 24 Stunden installiert, und die Infrastruktur wird kontinuierlich auf verdächtige Aktivitäten überwacht.

Zugangskontrolle und Sicherheitskultur

Der Zugang zu Systemen ist ausschliesslich qualifiziertem internen Personal gestattet, mit verschlüsselten Zugangsdaten und gesicherten Passwortspeichern.
Unternehmens-E-Mails werden nicht auf mobilen Geräten verwendet, und es werden keine Cloud-Mail-Plattformen (wie Gmail oder Office 365) eingesetzt.

Innovando GmbH pflegt eine **proaktive Sicherheitskultur**, in der jeder Mitarbeitende den Datenschutz nicht als Einschränkung, sondern als ethische und reputationsrelevante Verantwortung versteht.

Umweltrisiko

Die geografische Lage und Infrastruktur der Rechenzentren gewährleisten einen hohen Schutz gegen physische Risiken wie Brand, Überschwemmung oder extreme Wetterereignisse.
Die Partneranlagen sind ISO 27001 zertifiziert und gewährleisten Geschäftskontinuität auch unter kritischen Bedingungen.
Das Risiko eines Datenverlusts durch Umwelteinflüsse wird daher als **äusserst gering** eingestuft.

5. Risikoanalyse

Identifizierte potenzielle Risiken

- Unautorisierter Datenzugriff
- Zufälliger Datenverlust oder -beschädigung
- Unautorisierte Profilbildung
- Unrechtmässige Datenübermittlung

Gesamtrisiko-Bewertung
Dank der Infrastruktur, der Backup-Strategie und der internen Sicherheitsrichtlinien ist das **Restrisiko als äusserst gering bis vernachlässigbar** einzustufen.

6. Vorgehen bei Datenschutzverletzungen (Data Breach)

Im Falle einer vermuteten oder bestätigten Datenschutzverletzung wendet Innovando GmbH das folgende Verfahren an:

1. **Sofortige schriftliche Benachrichtigung** des Verantwortlichen;
2. **Technische Analyse innerhalb von 24 Stunden** zur Beurteilung des Umfangs und der Art des Vorfalls;
3. **Isolierung des betroffenen Systems**, um eine Ausbreitung zu verhindern;
4. **Unverzügliche Benachrichtigung** der betroffenen Personen und gegebenenfalls der zuständigen schweizerischen und europäischen Aufsichtsbehörden;

5. **Erstellung eines Vorfallsberichts**, der vertraulich archiviert und jährlich überprüft wird.

7. Gesamtauswertung der Auswirkungen

Die Gesamtauswertung berücksichtigt technische, organisatorische und menschliche Faktoren und bietet eine ganzheitliche Sicht auf den Datenschutzstatus des Unternehmens.

Methodische Analyse

Jede Verarbeitungstätigkeit wurde anhand von vier Parametern bewertet:

1. **Eintrittswahrscheinlichkeit** (Häufigkeit eines potenziellen negativen Ereignisses);
2. **Schwere des Einflusses** (möglicher Schaden für Rechte und Freiheiten);
3. **Wirksamkeit der Sicherheitsmassnahmen**;
4. **Reaktions- und Wiederherstellungsfähigkeit (Resilienz)**.

Die Analyse zeigt, dass das **Restrisiko äusserst gering** ist, da physische Redundanz, logische Segmentierung und interne Governance eine Gefährdung weitgehend ausschliessen.

Bewertung der Restrisiken

- **Datenverlust oder -beschädigung:** gemindert durch 3–2–1-Backup, RAID-5-Redundanz und Integritätsprüfungen.
- **Unautorisierter Zugriff:** gemindert durch Verschlüsselung, Firewalls und fehlenden mobilen Zugriff.
- **Unautorisierte Profilbildung:** ausgeschlossen, da Innovando keine automatisierten Entscheidungsprozesse einsetzt.
- **Menschlicher Fehler:** gemindert durch interne Richtlinien und begrenzte Zugriffsrechte.
- **Umweltereignisse:** minimales Risiko dank zertifizierter Infrastruktur und Redundanz.

Schlussfolgerung der Bewertung

Unter Berücksichtigung aller getroffenen Massnahmen, der Reife der internen Prozesse und der Sensibilisierung des Personals wird der Einfluss der Datenverarbeitung auf die Privatsphäre und die Rechte der Personen als **vernachlässigbar** eingestuft.
Es bestehen keine Szenarien, die gemäss Artikel 35 DSGVO oder dem Schweizer DSG als Hochrisiko gelten würden.

Innovando GmbH pflegt eine proaktive und dokumentierte Sicherheitsstrategie, bei der Datenschutz nicht nur als gesetzliche Verpflichtung, sondern als kontinuierliches Engagement für Integrität und Vertrauen verstanden wird.

8. Überprüfung und Aktualisierung

Diese DPIA wird **jährlich überprüft** oder bei wesentlichen Änderungen der Geschäftsprozesse, IT-Systeme oder geltenden Vorschriften angepasst.
Eine englische Kurzversion wird auf der offiziellen Website von Innovando Swiss veröffentlicht; das vollständige Dokument (diese Version) steht als PDF zum Download bereit und wird Kundenverträgen beigelegt.

9. Genehmigung

Genehmigt durch:
Andreas Arno Michael Voigt
CEO, Innovando GmbH
Verantwortlicher für die Datenverarbeitung

In Zusammenarbeit mit:
Sven Holzhuber
Technischer Leiter und Informationssicherheitsbeauftragter

Datum: 17.10.2025
Ort: Gonten, Schweiz