INNOVANDO
THE SWISS BRANDING COMPANY

Data Protection Impact Assessment (DPIA)
Legal reference: Article 35 EU Regulation 2016/679 (GDPR) – Swiss Federal Act on Data Protection (FADP, revised 2023)

Introduction

This *Data Protection Impact Assessment* (DPIA) is issued by **Innovando GmbH (operating as Innovando Swiss)** to evaluate and document the impact of personal data processing activities within its operational, consulting, and digital environments.
The purpose of this document is to transparently demonstrate compliance with the principles of *accountability*, *privacy by design*, and *privacy by default*, ensuring that all processing is carried out with full respect for the fundamental rights and freedoms of natural persons.

The DPIA also functions as a governance and prevention instrument: it allows for early identification of potential risks, an assessment of their likelihood and impact, and the implementation of appropriate technical and organizational measures.
Innovando GmbH is committed to maintaining a high standard of data protection based on information security, confidentiality, integrity, and responsible data management.

1. Data controller and operational context

Data controller
Andreas Arno Michael Voigt
Innovando GmbH
Loretto 4, 9108 Gonten (Switzerland)
Tel. +41 71 794 1500
Email: privacy@innovando.swiss

Technical and information security manager
Sven Holzhuber, appointed May 2, 2018

Data Protection Officer (DPO)
Not appointed, as it is not mandatory under the FADP or GDPR due to the scale and nature of the processing activities.

Purpose of processing
The processing of personal data serves the purposes of analytics, marketing, CRM, regular and extraordinary website maintenance, the production of strategic communication materials for client companies, and the administrative management of commercial relationships.

Data subjects
Clients, prospects, suppliers, employees, and website users.

Categories of personal data
Name, surname, company name, address, email, contractual data, invoicing data, cookies, and browsing data.

2. External processors and infrastructure

External processors

- **Metanet AG**, provider of cloud and hosting services (servers located in Switzerland, ISO 27001 certified).
- **BREVO**, newsletter management platform.
- **Banca Popolare di Sondrio**, banking services provider.
- **PayPal**, electronic payments platform.
- **BEXIO**, accounting software provider.

Certifications

- Partner data centers GTT (Interroute) and Equinix comply with ISO 27001 international information security standards.
- Innovando GmbH holds *Swiss Digital Services* and *Swiss Label* certifications.

Data localization
All data are processed and stored **exclusively within Switzerland**.
No data transfers are made to countries outside the EU or the European Economic Area that do not adhere to the GDPR or Swiss FADP.

3. Description of processing activities

Data collection methods
Data are collected through online forms, newsletters, cookies, contact forms, analytical tracking, event registrations, interviews, and, when necessary, manual collection.

Purpose of processing
Communication with clients and suppliers, traffic analysis, personalization of generated content, remarketing activities, and continuous improvement of services.

Tools and systems used
Google Analytics, Meta Pixel, CRM systems, and AI tools compliant with the *EU AI Act*, as declared in the *Declaration on the Use of Artificial Intelligence* published on the official website.

Data retention period
Data are stored for as long as necessary to carry out the assigned tasks, plus one additional year for

operational purposes.
Prospect data are deleted automatically after one year from collection.

4. Security measures and risk mitigation

Data security at Innovando GmbH is built upon a multilayered strategy grounded in the principles of *defense in depth* and *resilience by design*. Each system component is designed to guarantee operational continuity even in the event of hardware failure, human error, or external disruption.

Backup system and the 3–2–1 rule

Innovando fully applies the **3–2–1 backup rule**, an internationally recognized best practice that requires:

- **3 total copies of the data** (1 primary and 2 backups);
- **2 different storage media**, to reduce the risk of simultaneous failure;
- **1 copy stored off-site**, physically separated from the production environment.

In practice, company data are duplicated daily on a **primary NAS system configured in RAID 5** and on a **secondary NAS**, also in RAID 5, located in a separate physical unit.
Both backup sets are encrypted and undergo regular integrity tests. This architecture ensures that, even in the event of hardware damage, physical incident, or natural disaster, data loss is **virtually impossible**.

Encryption and data integrity

All backups are encrypted using advanced AES-256 encryption algorithms, and encryption keys are stored in isolated environments accessible only to authorized personnel.
Data integrity is continuously verified through hash checks and automated verification procedures to prevent silent data corruption.

Firewalls, segmentation, and updates

The corporate network is protected by **dedicated hardware firewalls** that segment network traffic and block unauthorized communications.
Servers are updated promptly, with security patches applied within 24 hours of release. The infrastructure is continuously monitored to detect unusual activity or access attempts.

Access control and security culture

Access to systems is limited to qualified internal personnel, with encrypted credentials and passwords stored in a secure vault.
Corporate email is not used on mobile devices, and no cloud-based email platforms (e.g., Gmail, Office 365) are employed, thereby eliminating synchronization and interception risks.

Innovando GmbH fosters a **proactive security culture**, where every collaborator understands data protection not as a constraint but as an ethical and reputational commitment.

Environmental risk

The geographic location and infrastructure of the data centers ensure a high level of protection against physical threats such as fire, flooding, and severe weather events.
Partner facilities are ISO 27001 certified and designed for business continuity under critical conditions. The risk of data loss from environmental causes is therefore classified as **extremely low**.

5. Risk assessment

Identified potential risks

- Unauthorized access to data
- Accidental loss or corruption of data
- Unauthorized profiling
- Unlawful data transfer

Overall risk assessment
Due to the company's infrastructure, backup systems, and strict internal policies, the overall residual risk is **extremely low to negligible**.

6. Data breach response procedure

In the event of a suspected or confirmed data breach, Innovando GmbH implements the following protocol:

1. **Immediate written notification** to the Data Controller;
2. **Technical assessment within 24 hours** to evaluate the nature and scope of the incident;
3. **Isolation of the affected system** to prevent further damage;
4. **Prompt communication** to affected individuals and, where necessary, to the Swiss and EU supervisory authorities;
5. **Incident report** documented and archived for annual review.

7. Overall impact assessment

The overall impact assessment integrates technical, organizational, and human factors, providing a holistic view of the company's data protection posture.

Methodological analysis

Each processing operation has been evaluated across four parameters:

1. **Likelihood of occurrence** (probability of a negative event);
2. **Severity of impact** (potential harm to individual rights and freedoms);
3. **Effectiveness of implemented safeguards**;
4. **Capacity for response and recovery (resilience)**.

This analysis concludes that the **residual risk** is extremely low, as physical redundancy, logical segmentation, and internal governance significantly minimize any potential impact.

Residual risk evaluation

- **Data loss or damage:** mitigated by 3–2–1 backups, RAID 5 redundancy, and integrity checks.
- **Unauthorized access:** mitigated by encryption, firewalls, and absence of mobile access.
- **Unauthorized profiling:** excluded, as Innovando does not engage in predictive or automated decision-making.
- **Human error:** mitigated by internal policies and restricted access privileges.
- **Environmental events:** minimal risk, thanks to certified infrastructure and redundancy.

Impact conclusion

Considering all implemented measures, process maturity, and staff awareness, the impact of data processing on individuals' privacy and rights is **negligible**.
No scenarios qualify as high-risk under Article 35 of the GDPR or the Swiss FADP.

Innovando GmbH maintains a proactive and documented security stance, treating data protection not merely as a regulatory requirement but as a continuous commitment to integrity and trust.

8. Review and update

This DPIA is subject to **annual review** or whenever substantial changes occur in business processes, IT systems, or relevant regulations.
A summarized English version will be published on the official Innovando Swiss website, while the full document (this version) will be available as a downloadable PDF and attached to client contracts.

9. Approval

Approved by:
Andreas Arno Michael Voigt
CEO, Innovando GmbH
Data Controller

In collaboration with:
Sven Holzhuber
Technical and Information Security Manager

Date: 17.10.2025
Location: Gonten, Switzerland