COMPLIANCE GUIDE · SWISS SMEs

Compliance Checklist

Ten practical steps to align your IT and data protection practices with the GDPR and the revised Swiss nFADP.

GDPR · EU Regulation 2016/679 Swiss nFADP

AVENUE DE LA GARE 46B – 1920 MARTIGNY
AVENUE LOUIS-CASAÏ 71 – 1216 COINTRIN
MAIL@AWSMTECH.CH – WWW.AWSMTECH.CH – +41 (0)22 552 60 70

Why this checklist

Below is a checklist of key steps and practices to help ensure GDPR and nLPD compliance. Swiss SMEs can use it as a working reference to review their IT and data protection readiness.

Each step corresponds to an essential aspect of GDPR / nFADP compliance. Following the checklist in order lets your organisation systematically address its obligations, from foundational governance through to continuous improvement.

01 – 03	**FOUNDATIONS**	The foundation: responsibility, awareness, transparency.
04 – 05	**SECURITY & DATA**	Security and data management within IT operations.
06	**THIRD PARTIES**	Vendor compliance — an often-overlooked area.
07	**BREACH READINESS**	Readiness for the worst-case scenario of a breach.
08	**INDIVIDUAL RIGHTS**	Making sure individual rights can be respected in practice.
09 – 10	**PEOPLE & CONTINUITY**	The human factor and the continuous nature of compliance.

HOW TO USE THIS GUIDE

Work through the ten steps with your IT lead and management team. Each card on the following pages states the action and what “done” looks like in practice — use it to audit where you stand today.

Steps 01–06

01 FOUNDATIONS

Assign Responsibility

Designate a person or team for data protection compliance — a privacy officer or coordinator. Make sure management supports compliance efforts and understands its accountability.

02 FOUNDATIONS

Map Your Data

Create a detailed map of personal data across your IT systems. Identify what data you hold, where it is stored, how it flows, and who has access. Record the purpose and lawful basis for each processing activity.

03 FOUNDATIONS

Update Privacy Notices

Keep clear, up-to-date privacy notices informing customers and employees about data collection, use, retention, and their rights. Make them easy to find — on your website, for example.

04 SECURITY & DATA

Implement Security Measures

Apply appropriate IT security controls: access restrictions, strong authentication, encryption of data at rest and in transit, and network security such as firewalls and anti-virus. Establish secure backup routines and a disaster-recovery plan.

05 SECURITY & DATA

Establish Retention Rules

Set and document retention periods for each data type. Configure systems to delete or archive data once those periods expire, using secure erasure. Never retain personal data longer than necessary.

06 THIRD PARTIES

Manage Third-Party Risk

Review every service provider and partner who handles personal data. Sign Data Processing Agreements that include GDPR / nLPD clauses, use standard contractual clauses for international transfers, and verify that processors maintain good security practices.

Steps 07–10

07 BREACH READINESS

Prepare for Breaches

Develop an incident-response plan that defines the steps to take on discovering a breach — containment, investigation, internal escalation — with ready templates for notifying the FDPIC, EU authorities, and affected individuals. Aim to report within 72 hours.

08 INDIVIDUAL RIGHTS

Enable Data Subject Rights

Set up procedures to log and respond to individuals' requests — access, correction, deletion, or objection — within the legal timeframe, typically 30 days under GDPR. Ensure IT can retrieve or delete data on request across every system.

09 PEOPLE & CONTINUITY

Train Employees

Conduct regular training on data-protection basics and your internal policies. Teach staff how to keep data secure — spotting phishing emails, for example — and how to handle privacy inquiries correctly.

10 PEOPLE & CONTINUITY

Monitor and Improve

Audit your compliance regularly. Keep processing records current, track KPIs such as incident counts and response times, and stay informed on regulatory changes. Treat data protection as an ongoing process, not a one-time project.

Where to go next

GOING FURTHER

Always refer back to authoritative resources for guidance. The official texts — the GDPR (EU Regulation 2016/679) and the Swiss nFADP — remain the primary references, and the FDPIC's website provides detailed summaries of the new law's provisions. Regulatory bodies such as the European Data Protection Board, the UK ICO, and the FDPIC also publish guides and FAQs that SMEs will find useful.

By staying informed through these sources and following this checklist, IT professionals and SME managers can confidently steer their organisation toward full GDPR and nLPD compliance — protecting client data and the business itself.

L’infogérance IT de confiance
pour les métiers sensibles.

AVENUE DE LA GARE 46B – 1920 MARTIGNY
AVENUE LOUIS-CASAÏ 71 – 1216 COINTRIN
MAIL@AWSMTECH.CH – WWW.AWSMTECH.CH – +41 (0)22 552 60 70