Compliance Checklist for Swiss SMEs

Below is a **checklist of key steps** and practices to help ensure GDPR and nLPD compliance, summarising the discussions above. SMEs can use this as a reference to review their IT and data protection readiness.

Each step bellow corresponds to an essential aspect of GDPR/nFADP compliance. By following this checklist, SMEs can systematically address their obligations:

- Steps 1–3 set the foundation (responsibility, awareness, and transparency).
- Steps 4–5 focus on **security and data management** within IT operations.
- Step 6 covers **vendor compliance**, an often-overlooked area.
- Step 7 readies the organisation for the worst-case scenario of a breach.
- Step 8 ensures **individual rights** can be respected in practice.
- Steps 9–10 emphasise the human factor and continuous nature of compliance.

Finally, always refer back to authoritative resources for guidance. The **official texts** – GDPR (EU Regulation 2016/679) and the **Swiss nFADP** – are primary references (the Swiss FDPIC's website provides detailed summaries of the new law's provisions). Regulatory authorities like the European Data Protection Board and national bodies (e.g. the UK ICO or FDPIC) publish guides and FAQs which can be very helpful for SMEs. By staying informed through these sources and following the strategies in this guide, IT professionals and SME managers can confidently steer their organisations toward full compliance with both GDPR and nLPD, thereby protecting their clients' data and their own business success.

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

1. Assign Responsibility

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

2. Data Inventory & Mapping

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

3. Update Privacy Notices

Ensure you have clear, up-to-date privacy notices/policies informing customers and employees about data collection, use, retention, and their rights. Make these easily accessible (e.g. on your website).

4. Implement Security Measures

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

5. Establish Data Retention Rules

Set and document retention periods for different data types. Configure systems to delete or archive data after these periods (with secure erasure). Don't retain personal data longer than necessary.

6. Manage Third-Party Risks

Review all service providers and partners who handle personal data. Sign Data Processing Agreements that include GDPR/nLPD clauses. Use standard contractual clauses for international data transfers when needed. Verify that processors maintain good security practices.

7. Prepare for Breaches

Develop an incident response plan. Define steps to take on discovering a data breach (containment, investigation, internal escalation). Include templates for notifying the FDPIC or EU authorities and affected individuals. Aim to report within 72 hours for safety.

8. Enable Data Subject Rights

Set up procedures to handle individuals' requests: data access, correction, deletion, or objection requests should be logged and responded to within the legal timeframes (typically 30 days under GDPR). Ensure IT can retrieve or delete data on request across all systems.

9. Train Employees

Conduct training for staff on data protection basics and your internal policies. Educate them on how to keep data secure (e.g. spotting phishing emails) and on proper procedures for handling personal data and privacy inquiries.

10. Continuously Monitor and Improve

Audit your compliance regularly. Keep the processing records updated with any new data or systems. Monitor key performance indicators like number of incidents or response times to requests. Stay informed on any regulatory changes or guidance updates. Treat data protection as an ongoing process, not a one-time project.