COMPLIANCE GUIDE

GDPR & nLPD

for Swiss SME IT infrastructures

2026 EDITION

COMPLIANCE GUIDE

CONTENTS

CONTACT

For any questions about this guide, please contact your AWSMTECH compliance representative.

PART ONE

THE ESSENTIALS

Everything you need to know on one page.

01 — WHY IT MATTERS

What the law requires of you

Swiss SMEs must comply with both the EU **GDPR** and the Swiss **Federal Act on Data Protection** (nLPD). These laws apply to all organisations processing personal data, regardless of size.

Non-compliance risks fines of up to **€20 million** under GDPR and **CHF 250,000** under nLPD, as well as significant reputational damage.

02 — KEY LEGAL PRINCIPLES

The four pillars of compliance

PRINCIPLE	DESCRIPTION
Lawfulness & transparency	Inform users clearly about data use and obtain valid consent.
Data minimisation	Collect only what is strictly necessary.
Security & confidentiality	Protect data through encryption, access control and incident response plans.
Accountability	Keep records, assign responsibility and train staff.

03 — IT COMPLIANCE CHECKLIST

Ten steps to secure your infrastructure

STEP	ACTION	OWNER
Assign responsibility	Appoint a privacy lead or DPO.	Management
Map data & risks	Audit data flows and assess gaps.	IT + Privacy
Legal basis & consent	Justify each data use (consent, contract, etc.).	Legal + IT
Update policies	Publish the privacy notice and internal guidelines.	Legal
Implement security measures	Encrypt data, enforce MFA, monitor systems.	IT Security
Retention & minimisation	Delete unnecessary data, set retention rules.	IT + Legal
Manage vendors	Sign Data Processing Agreements (DPAs).	Procurement
Enable rights requests	Allow users to access, correct or delete their data.	IT + Support
Train staff	Educate employees on privacy and security.	HR + IT

STEP	ACTION	OWNER
Breach response plan	Prepare and test incident response procedures.	IT + Privacy

04 — TECHNICAL MUST-HAVES

What your infrastructure must guarantee

ENCRYPTION **at rest & in transit**	**ACCESS CONTROL** **roles & MFA**	**RETENTION** **automated deletion**	**MONITORING** **incident detection**

05 — SWITZERLAND VS EU

Key differences to know

— Swiss law protects **individuals only**, not companies.

— Breach notification must be made **as soon as possible**, not within a fixed 72-hour window.

— Fines primarily target **responsible individuals**, not just companies.

— The legal basis is more flexible, but must **never infringe on privacy**.

PART TWO

THE GUIDE

Understand, implement, compare.

06 — OVERVIEW

GDPR and Swiss nLPD in a nutshell

GDPR (General Data Protection Regulation)

An EU-wide privacy regulation in effect since 2018, setting strict rules on how organisations handle personal data. GDPR has **extraterritorial reach**: it applies to companies outside the EU — including Swiss SMEs — if they offer goods or services to EU residents or monitor their behaviour online.

It mandates principles such as lawfulness, transparency, data minimisation, purpose limitation, accuracy, storage limitation, integrity/confidentiality and accountability (Article 5 GDPR). It introduces **data protection by design and by default**, mandatory breach notification within 72 hours, and substantial fines of up to €20 million or 4% of global turnover.

Swiss nLPD (new Federal Act on Data Protection, 2023)

Switzerland's updated data protection law, in force since 1 September 2023, aligns closely with GDPR's principles to maintain EU adequacy. It strengthens individuals' rights and introduces **Privacy by Design and Default** into Swiss law.

Key point: it **applies to the personal data of natural persons only** — unlike the old law, it no longer protects data belonging to legal entities. Swiss SMEs must comply even if they are not within GDPR's scope. The nLPD requires maintaining a record of processing activities (with some exemptions for low-risk SMEs) and “prompt” breach notification to the regulator.

Overlap and importance

Both GDPR and nLPD seek to protect personal data and give individuals control over their information. For a Swiss SME's IT department, this means **building an IT infrastructure that is compliant with both regimes at once**. A company that is GDPR-compliant will meet most nLPD obligations, as the Swiss law was designed to be compatible.

07 — COMPLIANCE REQUIREMENTS

Key compliance requirements for IT in SMEs

1. Lawful and transparent data processing

Every personal data processing activity must have a lawful basis and be transparent to the individual. GDPR defines six lawful bases (consent, contract, legal obligation, vital interests, public task, legitimate interests — Article 6). Swiss nLPD similarly requires justification for data processing.

Action for SMEs: document all categories of personal data your IT systems collect and process (customer data, employee data, etc.) and note the legal basis for each. Provide clear privacy notices to users. Avoid collecting data you don't need and only use it for the stated purposes. Your IT systems should be prepared to **fulfil data subject requests** (access, correction, deletion, portability).

2. Data storage and retention

Personal data should be stored securely and not retained longer than necessary. Under GDPR's “storage limitation” principle, data must be deleted or anonymised once it's no longer needed. Swiss nLPD expects the same behaviour.

Action for SMEs: implement retention policies — automatically delete or archive data after a defined period. Ensure backups and archives are also covered by these limits. If you use cloud services abroad, confirm that international transfers

comply with GDPR/nLPD rules (adequacy decision or standard contractual clauses). Document the retention period for each data category in your processing register.

3. Access control and data security

Both GDPR and nLPD mandate protecting personal data against unauthorised access, loss or breach — the "integrity and confidentiality" principle (Article 5(1)(f) and Article 32 GDPR), which requires **appropriate technical and organisational measures**.

Action for SMEs: restrict access on a need-to-know basis (role-based access control), enforce strong authentication (MFA), and keep systems patched. **Encryption** of data at rest and in transit is explicitly recommended under Article 32 GDPR: encrypted databases, HTTPS for all transmissions. Swiss nLPD requires similar minimum security standards. Also maintain anti-malware protection and a disaster recovery plan.

4. Breach notification and response

Despite best efforts, data breaches can happen. **Under GDPR**, any breach likely to pose a risk to individuals' rights must be reported to the supervisory authority **within 72 hours** of discovery. **Under Swiss nLPD**, breaches must be reported to the Federal Data Protection and Information Commissioner (FDPIC) **"as soon as possible"** where there is a high risk to the personality or fundamental rights of data subjects — with no fixed hour count, but no unjustified delay.

Action for SMEs: establish an **incident response plan** — procedures for identifying and investigating breaches, a clear internal reporting chain, and a template for notifying the regulator. Train staff to recognise incidents. If you miss the 72-hour GDPR window, you must justify the delay; affected individuals may also need to be informed if the breach is serious (Article 34).

5. Accountability and documentation

Compliance is not a one-off task — both GDPR and nLPD require ongoing **accountability**, meaning you should be able to demonstrate compliance at any time. GDPR Article 30 requires controllers to keep a **Register of Processing Activities (RoPA)**, with a possible exemption for enterprises with fewer than 250 employees whose processing is low-risk or occasional. The new Swiss law also makes a processing register mandatory, with a comparable exemption.

Action for SMEs: build a data processing inventory — purpose, data types, categories of individuals, external recipients, retention period, security measures applied. Define internal policies (IT security, data protection) and train staff. Assign responsibility for compliance — nLPD does not mandate a DPO, but the practice is recommended. Regularly audit and update your documentation.

08 — PRACTICAL STRATEGIES

Practical strategies for IT teams

Implementing GDPR and nLPD can seem daunting, but a set of concrete strategies turns legal mandates into everyday IT practice.

Data mapping & classification

Start with a **data map**: identify every place your SME's IT infrastructure stores or transmits personal data (databases, file servers, employee laptops, cloud services, email systems). Classify data by sensitivity. This mapping underpins every other step and reveals cross-border flows relevant to GDPR or nLPD.

Apply Privacy by Design

Build privacy and security into IT projects from the outset: fine-grained access control, encryption, the ability to delete or export data. Default settings should be privacy-friendly. Conduct a **Data Protection Impact Assessment (DPIA)** for any high-risk processing, as required by GDPR.

Strong encryption everywhere

Encryption makes data unreadable without the key — a critical safeguard against breaches. Encrypt data **at rest** (disks, databases, backups) and **in transit** (TLS/SSL, VPN, sensitive email). Manage keys separately from the data. Authorities often treat encryption as a mitigating factor during investigations.

Secure backups and recovery

Maintain **regular backups**, encrypted and protected by access controls. Test them periodically to confirm you can actually restore data. A robust backup system lets you restore personal data promptly after an incident, as GDPR and nLPD both expect.

Access management and monitoring

Set up a process to grant and revoke access rights (IAM), enable logging on systems with sensitive data, and regularly review user privileges under the least-privilege principle. **Encryption + access control + monitoring** form the triad of data security.

Vendor and partner management

Any processor handling data on your behalf must be covered by a **Data Processing Agreement (DPA)** in line with GDPR Article 28. Use standard contractual clauses for transfers outside an adequate jurisdiction, assess vendor security (ISO 27001, questionnaires), and limit the data you share to the necessary minimum.

Training and policies

Technology alone isn't enough: train staff on data protection best practices, on handling data-deletion requests, and on reporting incidents. An informed team strengthens your IT measures and reduces the risk of human error.

By implementing these strategies, IT teams in SMEs create an environment where compliance is part of day-to-day operations — not a last-minute fix.

09 — COMPARISON

GDPR vs nLPD: differences and overlaps

While GDPR and the Swiss nLPD share the same spirit and most of their requirements, a few important distinctions are worth knowing, especially for IT and compliance teams.

Scope of application

Both laws protect the data of **natural persons**. GDPR applies to any organisation processing data of EU residents, wherever it is based. The nLPD applies mainly to processing carried out in Switzerland or affecting people in Switzerland. New in nLPD: it no longer protects data belonging to **legal entities**, unlike the old Swiss law.

Regulatory authority and fines

GDPR provides for administrative fines of up to **€20 million or 4% of global turnover**, imposed by the authorities of each EU country. The nLPD caps fines at **CHF 250,000**, generally directed at **responsible individuals** rather than the company itself; the FDPIC does not issue fines directly, with serious cases potentially referred to criminal prosecution.

Breach notification window

GDPR sets a clear **72-hour** deadline after discovery of a breach. The nLPD requires notification **"as soon as possible"** where there is a high risk — a more flexible but equally urgent standard in practice. It is advisable to aim for a similar 72-hour window in both cases.

Data Protection Officer (DPO)

GDPR **requires a DPO** for certain organisations (public authorities, large-scale monitoring, sensitive data processing — Article 37). The nLPD **does not require a DPO**, but allows the voluntary appointment of a data protection advisor, which is recommended practice.

Processing records and SMEs

Both laws require a register of processing activities, with comparable exemptions for small, low-risk organisations. In practice, GDPR compliance on this point covers most nLPD obligations.

Individual rights and consent

The rights granted to individuals (access, rectification, deletion, objection, portability) are **very similar** between GDPR and nLPD, the latter having aligned its standards with GDPR. Some nuances exist around consent for high-risk profiling.

International data transfers

GDPR restricts transfers outside the EU/EEA unless there is adequate protection or appropriate safeguards (standard contractual clauses, binding corporate rules). The nLPD applies a comparable logic, with a list of adequate countries largely aligned with the EU's. The EU and Switzerland mutually recognise each other as offering adequate protection.

In summary, GDPR and nLPD have more in common than they have differences. The core principles — lawfulness, transparency, security, individual rights — and the operational tasks are, in essence, the same. It's sensible to align with the stricter version of each requirement: apply GDPR's 72-hour rule in all cases, and keep 4% of turnover in mind as the risk ceiling.