GDPR & nFADP Guide for Pros

AVENUE LOUIS-CASAÏ 71 – 1216 COINTRIN
MAIL@AWSMTECH.CH – WWW.AWSMTECH.CH

GDPR & Swiss nLPD Compliance for SME IT Infrastructures

✅ Why It Matters

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 (up to €20M under GDPR, CHF 250k under nLPD) and reputational damage.

🔍 Key Legal Principles

Principle	Description
Lawfulness & Transparency	Inform users clearly about data use and obtain valid consent.
Data Minimisation	Collect only what's necessary.
Security & Confidentiality	Protect data with encryption, access controls, and breach response plans.
Accountability	Keep records, assign responsibility, and train staff.

🛠️ IT Compliance Checklist

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 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
Breach Response Plan	Prepare and test incident response procedures.	IT + Privacy

🔐 Technical Must-Haves

- Encryption: For data at rest and in transit.

- Access Control: Role-based permissions, MFA.
- Retention Policies: Automate deletion of outdated data.
- Monitoring: Detect and respond to breaches swiftly.

CH Swiss vs EU Differences

- Swiss law protects individuals only, not companies.
- Breach notification must be done ASAP, not within 72h.
- Fines target individuals, not just companies.
- Legal basis is flexible, but must not infringe privacy.

RGDP Guide for the Professionals

A GDPR Compliance Guide for IT Infrastructures in Swiss SMEs (including Swiss nLPD)

Dual Regulation Compliance

Swiss SMEs must comply with both the EU's GDPR and Switzerland's new Federal Act on Data Protection (nLPD). GDPR can apply to Swiss businesses if they handle EU residents' data, while nLPD governs personal data processing on Swiss soil. Ignoring either law risks penalties and erodes customer trust.

Key IT Obligations

Both laws require **lawful & transparent data processing**, strong **security measures (access control, encryption)**, strict **data retention limits**, readiness for **breach notification**, and respect for individuals' data rights. IT teams play a crucial role in implementing these compliance measures.

Proactive Data Governance

Plan, Protect, Document: Map your data flows, enforce privacy by design, document processing activities, and continuously monitor compliance. A proactive approach not only avoids fines but also builds customer confidence and a future-proof IT environment.

Overview: GDPR and Swiss nLPD in a Nutshell

GDPR (General Data Protection Regulation) – An EU-wide privacy regulation effective 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/services to EU residents or monitor their behaviour online. GDPR mandates principles like lawfulness, transparency, data minimisation, purpose limitation, accuracy, storage limitation, integrity/confidentiality, and accountability (Article 5 GDPR). It introduced obligations such as **data protection by design and by default**, mandatory breach notifications within 72 hours, and substantial fines for non-compliance (up to €20 million or 4% of global turnover). For IT infrastructure, GDPR translates to ensuring that systems and processes protect personal data at all stages – from collection and storage to transfer and deletion

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. The nLPD (revised FADP) strengthens individuals' rights and introduces **Privacy by Design and Default** into Swiss law. Key points: it **applies to personal data of natural persons** (the new law, unlike the old one, no longer protects data on legal entities). Swiss SMEs handling personal data must comply with nLPD requirements even if they are not under GDPR scope. Notably, nLPD requires maintaining a record of processing activities (with some exemptions for low-risk SMEs) and "prompt" breach notification to the regulator. However, there are **some differences** from GDPR (detailed later): for example, fines under nLPD are capped at CHF 250,000 and typically target responsible individuals, and breach reports must be made "as soon as possible" rather than within a fixed 72-hour window.

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 a compliant IT infrastructure** that meets *both* sets of requirements. Fortunately, a company that is GDPR-compliant will meet most nLPD obligations, as the Swiss law was designed to be compatible. The following sections outline the core compliance requirements and practical steps for IT teams, and highlight where GDPR and nLPD converge or diverge.

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) for processing (Article 6 GDPR). 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 explaining what data is collected and why (transparency). Avoid collecting data you don't need (data minimisation) and only use it for the stated purposes. For instance, if an SME's website tracks user behaviour with analytics, GDPR likely requires user consent or another valid basis for that tracking. Both laws also enshrine individuals' rights (access, correction, deletion, data portability, etc.), so IT systems should be prepared to **fulfil data subject requests** – e.g. allowing extraction or deletion of a user's data upon request.

2. Data Storage and Retention

Personal data should be stored securely and not retained longer than necessary. Under the GDPR's "storage limitation" principle, data must be deleted or anonymised once it's no longer needed for the purpose collected. Swiss nLPD similarly expects you not to keep personal data indefinitely without reason. **Action for SMEs**: Implement retention policies in IT systems – e.g. automatically delete or archive data after a certain period if it's not needed. For example, logs containing personal data might be purged after X months. Ensure that backups and archives are also covered by these retention limits (so old personal data doesn't live forever in backup files). If your SME uses cloud services or data centers abroad, confirm that international storage complies with GDPR/nLPD transfer rules – i.e. either the country has an adequacy decision or you have safeguards like Standard Contractual Clauses. Document the retention period for each category of data in your processing register. By managing storage carefully, you reduce risk and comply with the obligation to only hold data as long as needed.

3. Access Control and Data Security

Both GDPR and nLPD mandate protecting personal data against unauthorised access, loss, or breach. This is the "integrity and confidentiality" principle (GDPR Article 5(1)(f)) and is elaborated in GDPR Article 32, which requires **appropriate technical and organisational measures** to secure data. In practice, this means SMEs must enforce strong **access controls** and cybersecurity measures in their IT infrastructure. **Action for SMEs**: Restrict access to personal data on a need-to-know basis – e.g. use role-based access control in databases and applications so that employees only see data necessary for their role. Implement authentication measures (strong passwords, multi-factor authentication) for systems that contain personal info. Regularly update and patch software to fix security vulnerabilities. **Encryption** should be used to protect data at rest and in transit: encrypted databases, laptops, and communications significantly reduce the risk of data being readable if compromised. In fact, encryption is explicitly recommended as an appropriate measure under GDPR (listed in Article 32) because it renders personal data unreadable to outsiders without the key. For example, a GDPR-compliant SME will encrypt customer data stored on a server, and use HTTPS for all data transmissions. Swiss nLPD also requires adherence to minimum data security standards (detailed in the implementing Ordinance) – effectively similar safeguards. IT teams should also maintain **systems integrity and availability**: ensure anti-malware is in place, and have disaster recovery plans. By fulfilling these security requirements, you not only comply with the law but also protect your business from incidents. (Both regulations consider security measures when evaluating liability – under GDPR regulators may be lenient if strong protection like encryption was in place during a breach.)

4. Breach Notification and Response

Despite best efforts, data breaches can happen (e.g. a hacker attack or even an employee error leading to exposure of personal data). GDPR and nLPD both impose a duty to report certain breaches to authorities. **Under GDPR**, any personal data breach that is likely to pose a risk to individuals' rights must be reported to the supervisory authority **within 72 hours** of discovery. For example, if a database of customer data is stolen, the company must notify its EU country's Data Protection Authority (DPA) within 72 hours, outlining the nature of the breach and mitigation steps. **Under Swiss nLPD**, breaches must be reported to the Federal Data Protection and Information Commissioner **"as soon as possible"** if the breach could result in a high risk to the personality or fundamental rights of the data subjects. The Swiss law doesn't set an exact hour count, but the intent is to notify without delay. **Action for SMEs**: Establish an **incident response plan**. This includes procedures for identifying and investigating suspected breaches, a clear internal reporting chain (e.g. IT staff report immediately to security officer or management), and a template for notifying the regulator. Train your team to recognise incidents. Keep in mind that under GDPR if you miss the 72-hour window, you must provide justification for the delay. You may also need to inform affected individuals if the breach is serious (GDPR Article 34). Having a well-tested response plan will ensure you can react quickly and comply with these notification requirements. Both laws treat breach response as critical – failing to notify when required can itself result in penalties.

5. **Accountability and Documentation**

Compliance isn't just a one-off task – both GDPR and nLPD require ongoing accountability. This means you should be able to demonstrate your compliance at any time. Key documentation for SMEs includes maintaining a **Register of Processing Activities (RoPA)** and written policies. GDPR Article 30 requires data controllers to keep records of what personal data they process, why, where it's stored, who it's shared with, etc., unless an enterprise has fewer than 250 employees *and* the processing is low-risk/occasional (many SMEs might qualify for this exemption, but if you handle sensitive data or frequent processing, you likely still need a record). The new Swiss law makes a processing register mandatory as well, with an exemption for SMEs <250 employees if the processing poses minimal risk. **Action for SMEs**: Build and maintain a data processing inventory. List all your IT systems or databases that contain personal data and record details such as: purpose of processing, types of data, categories of individuals, any external recipients (e.g. cloud providers), retention period, and security measures applied. This inventory is not only a legal requirement but also immensely helpful for identifying compliance gaps. Additionally, define internal **policies** (e.g. an IT security policy, data protection policy) and train staff on them. Assign responsibility for data protection compliance (it could be an internal privacy officer or an external consultant – while nLPD does not force SMEs to appoint a Data Protection Officer, having a designated person is recommended). Regularly audit and update your documentation. By keeping thorough records and policies, you satisfy the accountability principle and are prepared if regulators or clients ask to see your compliance efforts.

Practical Implementation Strategies for IT Teams

Implementing GDPR and nLPD requirements can seem daunting, but a set of concrete strategies will help turn legal mandates into actionable IT practices:

- **Data Mapping & Classification**: Start with a **data map**. Identify all places where your SME's IT infrastructure stores or transmits personal data: databases, file servers, employee laptops, cloud services, email systems, etc. Classify the data by sensitivity (e.g. public, internal, confidential, highly sensitive). This mapping underpins all other steps – you can't protect or regulate data if you don't know where it is. A thorough data map helps in meeting both GDPR and nLPD obligations by revealing what data falls under which law (EU or Swiss) and highlighting cross-border data flows.
- **Apply Privacy by Design**: Incorporate privacy and security considerations into IT projects from the outset. This means when designing or choosing software for, say, a new customer management system, ensure it has necessary privacy features (like fine-grained access control, encryption, and the ability to delete or export data). Privacy by design and default is explicitly required by both

GDPR and the nLPD. For example, default settings should be privacy-friendly (e.g. analytics off unless enabled). Conduct a **Data Protection Impact Assessment (DPIA)** for any new system or process that could be high-risk (GDPR requires DPIAs for high-risk processing like large-scale use of sensitive data or systematic monitoring). IT teams should have a DPIA template and know when to trigger this process. By embedding privacy controls early, you prevent costly re-engineering later and demonstrate compliance commitment.

- **Strong Encryption Everywhere**: Use encryption as a fundamental tool to protect data. As noted, encryption protects data by making it unreadable without the decryption key – a critical safeguard against breaches. Implement encryption for data **at rest** (e.g. full-disk encryption on servers and laptops, database encryption features, encrypted backups) and **in transit** (TLS/SSL for web traffic, VPN for remote access, encrypted email for sensitive info). Modern cloud services often provide encryption options – ensure they are enabled. Remember that encryption keys must be managed securely (keep keys safe and separate from the data). By encrypting personal data, even if your system is hacked or a laptop is lost, the risk to individuals is greatly reduced. Both laws implicitly favor encryption – under GDPR, authorities may consider your use of encryption as a mitigating factor during investigations. In practice, SMEs should encrypt customer databases, employee personal folders, and any portable media. It's one of the most effective ways IT can prevent unauthorised data access.

- **Secure Backups and Recovery**: Maintain regular **backups** of personal data, but do so securely. Backups are essential for the availability aspect of data protection – if data is accidentally deleted or ransomware encrypts your systems, you must be able to restore access to avoid permanent loss (a requirement under the security principle to ensure availability). **Action**: Set up automated backups for critical systems containing personal data (customer databases, etc.) on a secure secondary location. Encrypt backup files or drives as well, since they contain the same sensitive data. Protect backup storage with access controls. Test your backups periodically to confirm you can actually restore data in an emergency. Having timely backups also factors into incident response; for instance, if a breach corrupts data, you can recover clean data from backups, possibly negating the need to notify data subjects if you can confirm no data was exfiltrated. Both GDPR and nLPD expect that organisations can **restore personal data in a timely manner after incidents**, which is exactly what a robust backup system enables. Don't forget to include email and document systems in your backup plan if they contain personal info, and define retention periods for backups to align with overall data retention policies.

- **Access Management and Monitoring**: Implement tools for managing user access rights and monitoring usage. For example, use an Identity and Access Management (IAM) system or at least a documented process to approve and revoke employee access to systems with personal data if their role changes or they leave. Enable logging on systems to record who accessed or modified sensitive data and when – this helps in audits and in forensic analysis if something goes wrong. Regularly review user accounts and privileges (least privilege principle). Consider using intrusion detection systems or at least monitor system logs for unusual access patterns which might indicate a breach. Under GDPR's accountability, you should be able to show you have control over who can do what with personal data. For SMEs with limited IT admins, even simple measures like strong unique passwords for each employee and not sharing accounts will go a long way. **Encryption + Access Control + Monitoring** form a triad of security that covers confidentiality, integrity, and availability.

- **Vendor and Partner Management**: SMEs often rely on third-party services or vendors (cloud hosting providers, SaaS tools, IT support companies) which might process personal data on their behalf. Under GDPR, whenever a data controller (your company) uses a data processor (a vendor) to handle personal data, you **must have a Data Processing Agreement (DPA)** in place that imposes GDPR-equivalent obligations on the processor (see GDPR Art. 28). Similarly, Swiss SMEs should

ensure vendors comply with nLPD. **Action**: Inventory all external providers that handle your personal data (e.g. an email marketing service with your client list, or an HR payroll service with employee data). For each, ensure there's a contract or DPA that covers data protection responsibilities, confidentiality, and breach notification duties. Use standard contractual clauses (SCCs) if transferring personal data from Switzerland/EU to a country without an adequacy decision. Evaluate vendors' security measures – you can use security questionnaires or request certifications (like ISO 27001 or adherence to a code of conduct). Choose reputable providers with strong privacy reputations. Also, limit what data you share with them to the necessary minimum. Periodically review these processors: for critical vendors, you might do an annual check-in or ask for updated compliance info. Effective vendor management ensures that your compliance efforts are not undermined by a third party. Remember, under GDPR you are still accountable to individuals for what your processors do with the data, and under nLPD your company's leadership could be personally liable if a partner misuses data. So treat vendor relationships as an extension of your IT compliance program.

- **Training and Policies**: Technology alone isn't enough – staff awareness is key. Provide training to employees about data protection best practices and your policies. For instance, train them not to click suspicious links (to prevent breaches) and how to handle personal data queries from customers. Establish clear procedures, such as what to do if someone requests their data to be deleted (data subject right) or how to report a lost device. Both GDPR and nLPD foster a culture of data protection, and regulators often check if companies have taken steps to educate staff. An *informed team* will support your IT measures and reduce human error risks. Consider short periodic refreshers or including data protection topics in onboarding for new hires.

By implementing these strategies, IT teams in SMEs create an environment where compliance is built into day-to-day operations. The goal is to make privacy and security a default part of the infrastructure – not an afterthought. This proactive stance will greatly reduce the likelihood of incidents and will put the company in a strong position if audited by authorities or asked by business partners about compliance.

GDPR vs. nLPD: Differences and Overlaps

While GDPR and the Swiss nLPD share the same spirit and many requirements, there are a few important distinctions to be aware of. The following highlights key differences and overlaps between the two laws, especially relevant to IT and compliance efforts:

- **Scope of Application**: Both laws protect personal data of **natural persons** (individuals). GDPR applies to organisations of any size worldwide if they process personal data of people in the EU (thus catching Swiss companies with EU customers). The nLPD applies primarily to processing carried out in Switzerland or affecting individuals in Switzerland. One notable change in the new nLPD is that **data about legal entities (companies) is no longer protected**, whereas the old Swiss law did protect it (GDPR never covered legal entities' data). In practice, most SMEs deal with individuals' data (customers, employees), so this change mainly reduces scope for B2B data like company registration information.

- **Regulatory Authority and Fines**: Enforcement mechanisms differ. Under GDPR, violations can lead to heavy **administrative fines on companies** – up to €20 million or 4% of annual global turnover, whichever is higher. These fines are imposed by Data Protection Authorities in each EU country. The Swiss nLPD, on the other hand, imposes fines up to **CHF 250,000**, and uniquely these fines are usually directed at **responsible individuals** (e.g. a company's leadership) rather than the company as a whole. In Swiss practice, the company might pay the fine on behalf of the individual, but legally it targets persons. Also, the Swiss Data Protection Commissioner (FDPIC) does not directly issue fines; serious cases may be referred for criminal prosecution. For SMEs, this means GDPR carries a risk of very large corporate fines, whereas Swiss law's penalties, though significant, are capped at

a lower amount and personal in nature. **Overlap**: In both regimes, failing to comply can result in financial penalties and reputational damage, so in either case it's vital to adhere to the rules.

- **Breach Notification Window**: GDPR specifies a clear deadline – a breach must be reported to the supervisory authority within **72 hours** after the controller becomes aware of it (unless the breach is unlikely to harm individuals). The Swiss nLPD requires notifying the FDPIC **"as soon as possible"** in the event of a breach that poses a high risk to the data subjects. This is a slightly more flexible but also somewhat vague standard – essentially, do not delay notification unreasonably. In practice, companies in Switzerland should treat the timing with equal urgency; it's wise to aim for a similar 72-hour timeframe for Swiss breaches as well. One difference: under nLPD, if a breach is not likely to result in a "high risk" to individuals, notification might not be mandatory, whereas GDPR's threshold is "risk" (any risk, not high) to individuals' rights and freedoms as the trigger for notifying authorities. Both laws also expect documentation of breaches and remedial actions taken.

- **Data Protection Officer (DPO)**: GDPR **requires appointing a DPO** for certain organisations – for example, public authorities or companies that do large-scale monitoring or process a lot of sensitive data (Article 37 GDPR). Small SMEs often are exempt unless their core activities involve risky processing. The nLPD **does not mandate a DPO** by law. However, it allows voluntary appointment of a **Data Protection Advisor**, and it's recommended as a good practice especially if the company's data processing is complex. Many Swiss companies choose to designate someone (internally or an external consultant) to oversee privacy compliance even if not strictly required. Thus, having a DPO or privacy officer is an overlap in the sense of being beneficial under both regimes (and if you operate with EU data, you might need one for GDPR anyway).

- **Records of Processing & SMEs**: Both laws require maintaining a record of processing activities (the documentation of data flows we discussed). GDPR has an exemption for small organisations *only if* their processing is not likely to result in a risk to rights, is not frequent, and doesn't include special categories of data – which means many SMEs still need a record if they handle any sensitive data or do regular processing. The Swiss ordinance similarly provides an exemption for SMEs with under 250 employees if the processing is low-risk. **Overlap**: In effect, most businesses benefit from keeping these records regardless of the formal exemption, as it's fundamental to demonstrating compliance. If you've complied with GDPR's documentation, you've essentially complied with nLPD's on this point.

- **Individual Rights and Consent**: The rights given to individuals (like access to their data, the right to correction, deletion, objection to processing, data portability, etc.) are **very similar in GDPR and nLPD**. Swiss law aligned these rights with the GDPR standard. One minor difference is how consent and legitimate interest might be balanced: GDPR requires explicit consent for processing sensitive personal data, whereas nLPD also requires consent for "high risk profiling" and has some nuances on legitimate interest. But these are fine-grain details; an SME that handles data ethically – obtaining consent when required, honouring opt-outs, and responding to requests – will satisfy both regimes. Both laws also require transparency about data processing and typically require a privacy notice to be provided to individuals when collecting their data.

- **International Data Transfers**: GDPR restricts transfers of personal data to countries outside the EU/EEA that don't have adequate data protection laws, unless appropriate safeguards (like European Commission-approved Standard Contractual Clauses or Binding Corporate Rules) are in place. The nLPD has a comparable rule: personal data may only be transferred abroad if the destination country is deemed to have adequate protection or if safeguards are used. The Swiss Federal Council maintains a list of countries considered adequate, which is largely in sync with the EU's list. The UK and EU are considered adequate from Switzerland's perspective, and vice versa Switzerland is considered adequate by the EU. For SMEs using cloud services or partners outside Switzerland, this means you should treat cross-border data flows similarly under both laws –

check if the country is on the approved list or use contractual clauses/consent. **Overlap**: Both frameworks aim to ensure personal data isn't sent to jurisdictions with weaker privacy protections without safeguards.

In summary, GDPR and the Swiss nLPD have more commonalities than differences. The core principles (lawfulness, transparency, security, individual rights) and the operational tasks (keeping records, securing data, managing breaches) are effectively the same. The differences lie in procedural details and enforcement approach – for instance, how and when to notify breaches and the scale of fines. Swiss SMEs that are already in line with GDPR will find they only need minor adjustments to fully comply with nLPD. It's wise to err on the stricter side of any difference (e.g. follow GDPR's 72-hour rule for breaches in all cases, and treat 4% of turnover as a potential maximum penalty to stay motivated). Being conscious of these nuances ensures that your compliance program covers both regimes thoroughly.

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