



GDPR & DSG Compliance Checklist

Data protection basics for small teams in Switzerland and the EU.

Version 1.0 · October 2026 · switech-solution.com

Since 1 September 2023, Switzerland's revised Federal Act on Data Protection (FADP, German: DSG) has been in force. It applies to any processing of personal data that has an effect in Switzerland, including by companies abroad.

The EU General Data Protection Regulation (GDPR) also applies to you if you have an establishment in the EU, or if you offer goods or services to people in the EU or monitor their behaviour (e.g. through tracking). The checklist names the relevant articles of both laws.

HOW TO USE THIS CHECKLIST

Work through the items in order and tick off what is done. Start with everything marked "Critical". Repeat the review before every major release and at least once per quarter.

Priorities: **CRITICAL** **IMPORTANT** **RECOMMENDED**

1 KNOW YOUR DATA

☐ Create a data map **CRITICAL**

Which personal data do you process, where is it stored, what is it used for, and who has access?

☐ Record of processing activities **IMPORTANT**

FADP Art. 12, GDPR Art. 30. In Switzerland, companies with fewer than 250 employees are usually exempt, unless they process sensitive data on a large scale or carry out high-risk profiling.

☐ Data minimisation and retention **IMPORTANT**

Collect only the data you need, define retention periods and set up a deletion process.

2 TRANSPARENCY

☐ Complete privacy policy **CRITICAL**

Controller and contact details, purposes, recipients, countries for transfers abroad including safeguards, and data subject rights. FADP Art. 19, GDPR Art. 13/14.

☐ Cookies and tracking **CRITICAL**

Switzerland: inform about cookies and allow users to refuse them (Art. 45c Telecommunications Act). EU: obtain active consent before setting non-essential cookies.

☐ Legal notice (imprint) **IMPORTANT**

Commercial websites must clearly state identity and contact address (in Switzerland Art. 3 para. 1 let. s UCA for online offers).

3 LEGAL BASIS & CONSENT

☐ GDPR: a legal basis for every processing **CRITICAL**

Each processing needs a basis under Art. 6, such as a contract, legitimate interest or consent.

☐ FADP: follow the principles **IMPORTANT**

The FADP does not require a legal basis for every processing, but compliance with its principles (Art. 6). Consent is required in certain cases, e.g. for sensitive personal data.

☐ Obtain consent correctly **IMPORTANT**

Voluntary, informed and documented, and revocable at any time. Double opt-in is recommended for newsletters.

4 SERVICE PROVIDERS & TRANSFERS ABROAD

☐ Data processing agreements **CRITICAL**

With every provider that processes personal data on your behalf (hosting, email, CRM, forms). FADP Art. 9, GDPR Art. 28.

☐ Check transfers abroad **CRITICAL**

Allowed to countries with adequate protection (Federal Council list or EU adequacy decisions) or with safeguards such as standard contractual clauses. USA: check whether the provider is certified under the Data Privacy Framework.

☐ Keep a list of providers **RECOMMENDED**

Maintain an up-to-date overview with purpose, data types and country.

5 DATA SECURITY

☐ Technical and organisational measures **CRITICAL**

Access control, encryption, backups, two-factor authentication, updates. FADP Art. 8, GDPR Art. 32.

☐ Privacy by design and by default **IMPORTANT**

Plan privacy-friendly defaults from the start. FADP Art. 7, GDPR Art. 25.

☐ Data protection impact assessment **IMPORTANT**

Carry one out in advance for processing that is likely to result in a high risk. FADP Art. 22, GDPR Art. 35.

6 DATA SUBJECT RIGHTS

☐ Answer access requests **CRITICAL**

Generally free of charge and within 30 days (FADP Art. 25, DPO Art. 18). GDPR: within one month (Art. 12, 15).

☐ Implement further rights **IMPORTANT**

Correction, erasure, objection and data portability (FADP Art. 28, GDPR Art. 20).

☐ Verify identity **IMPORTANT**

Before disclosing data, make sure the requesting person is the data subject.

7 DATA BREACHES

☐ Breach process **CRITICAL**

Detect, assess and document incidents. Define who decides and who communicates.

☐ Notify the FDPIC (Switzerland) **CRITICAL**

As soon as possible if the breach is likely to result in a high risk for the people affected. Inform those affected if necessary for their protection (FADP Art. 24).

☐ Notify the supervisory authority (EU) **CRITICAL**

Within 72 hours of becoming aware, unless the breach is unlikely to result in a risk (GDPR Art. 33).

8 ORGANISATION

☐ Responsibility and training **IMPORTANT**

Appoint a responsible person and train staff in handling personal data.

☐ EU representative **RECOMMENDED**

Without an EU establishment but with offers for people in the EU, a representative is usually required (GDPR Art. 27), with exceptions for occasional processing.

☐ Swiss representative **RECOMMENDED**

Foreign companies need a representative in Switzerland under certain conditions (FADP Art. 14).

☐ Annual review **RECOMMENDED**

Review the privacy policy, providers and processes at least once a year.

Sanctions: the FADP provides for fines of up to CHF 250,000, imposed on the responsible individuals for intentional violations. The GDPR provides for fines of up to EUR 20 million or 4% of worldwide annual turnover.

This checklist is not legal advice and does not replace an assessment of your specific case. Status: October 2026. The official texts are authoritative: FADP (SR 235.1) and DPO on fedlex.admin.ch, guidance from the FDPIC on edoeb.admin.ch, and the GDPR on eur-lex.europa.eu.

Questions or need support?

I help small businesses and founders build secure AI tools and automations. The intro call is free.

www.switech-solution.com