

Summary Checklist: Implementation of the New Swiss Data Protection Act

Note: The following focuses on most the relevant tasks for private companies who implement the new Swiss Data Protection Act (DPA), which will enter into force on September 1, 2023. The checklist is not comprehensive. Where the checklist refers to updates, the need for such depends upon existing documentation and relevant processing activities. There is no "one size fits all" implementation; the specific situation is to be taken into account.

1. Define **entities and processing activities** in scope of DPA and implementation project.
2. Evaluate **whether** and to what extent entities and processing activities identified above are **GDPR compliant** (if so, follow-up to implement the DPA may be limited).
3. Define **implementation project responsibilities**.
4. Define whether to appoint a **data protection advisor** under the DPA (not mandatory for most private companies, except where they execute tasks mandated by federal law).
5. Define whether there is a need to appoint a **Swiss representative** (for foreign companies).
6. Prepare **processing records** (exceptions apply for companies with less than 250 employees, as set forth in the Ordinance on the DPA).
7. Prepare **privacy policies** and similar information documents to inform data subjects about the processing of their personal data.
8. Review and update **data processing agreements** with third parties and templates for such data processing agreements.
9. Review and update **intragroup data transfer agreements**.
10. Review and update **other agreements** (with customers, suppliers, employees, etc.) in relation to data protection aspects.
11. Prepare **data protection impact assessments**; where needed, **consult with the Federal Data Protection and Information Commissioner** on these.
12. Review **cross-border transfers**, update related agreements and perform transfer impact assessment for transfers to third countries.
13. Review and update **technical and organizational data security measures**, determine whether there is a need to log access and define processing regulations and, if so, implement accordingly.
14. Review and update **data retention** policy and other data protection related policies.
15. Define process to comply with **data breach notification obligation**.
16. Review and update processes to comply with **data subject rights**.
17. Review and update **processes** to comply with other data protection requirements.
18. Define and implement **training** for employees.
19. Define process and responsibilities to **regularly review and update** compliance documentation.