



## A Wakeup Call – The New Swiss Data Protection Act Enters Into Force on September 1, 2023

[Sabrina Schnyder](#)

The Swiss Parliament approved the Federal Data Protection Act ([The Swiss Parliament Agrees on the Draft Bill of a New Data Protection Act](#)) in fall 2020. The Federal Office of Justice recently communicated that the new law will enter into force on September 1, 2023.

While some stakeholders have voiced disappointment that the date got further pushed back, there is also a positive note to the delay. The nDPA does not provide for a statutory transition period, which means that organizations subject to the nDPA have just over one year to implement the revised law. Experience from the General Data Protection Regulation (GDPR) has shown that the implementation process is time-consuming and companies should take advantage of the informal transition period and start the process now.

In addition, given the harsh criticism the draft Ordinance to the Data Protection Act (nDPAO) has elicited, hopes are high that the additional time will allow the Federal Council to put significant effort toward drafting a final version of the nDPAO that takes into consideration these comments.

### **Our company is already GDPR compliant; is there anything left to do?**

Companies that are already compliant with the GDPR will certainly have an advantage as the nDPA adopts many of the principles and obligations known under the GDPR. For further information we refer to our recent publication ([Part 2: Revised to Match the EU General Data Protection Regulation — or Almost](#)). In this case companies can build on the work done for compliance with the GDPR, start reviewing their existing GDPR documentation, and adapt it to Swiss law where necessary. In addition, where the GDPR goes beyond Swiss data protection law, companies will have to decide on whether they want to follow the stricter GDPR approach throughout or whether they want to adopt a more pragmatic and softer approach provided under Swiss law for their entities that are subject only to the nDPA.

### **Our company is not GDPR compliant. What now?**

For companies not yet compliant with the GDPR, we suggest the following approach:

- 1) **Data Flow Mapping:** Start identifying (1) the type of personal data that is processed, including any sensitive personal data, (2) where such personal data is stored, and (3)

who has access to that personal data internally and externally, including any access from abroad.

- 2) **Documentation:** Prepare nDPA-compliant documentation, such as inventories, privacy notices, necessary data impact assessments, and data transfer agreements.
- 3) **Technical and Organizational Measures:** Put in place internal policies and technical measures to sufficiently secure the personal data, including training any of your staff. Typical examples are data breach response plans and internal procedures on how to handle data access requests by data subjects.
- 4) **Data Protection Officer (DPO):** Consider appointing a DPO for your company or entity to ensure ongoing compliance with the nDPA.

## It's a lot. Where should we start?

In terms of priority, we recommend to focus on the obligations that are subject to criminal sanctions under the nDPA. Hence, a company should start by implementing the following:

- **Transparency Obligations:** privacy notices, in particular those publicly visible, for example, website privacy notices
- **Access Rights:** internal policies on how to respond to requests from data subjects
- **Outsourcing:** renew or conclude data processing agreements with third-party vendors
- **International Data Transfers:** identify data flows and the need to put in place Standard Contractual Clauses conduct any data transfer impact assessments
- **Data Security:** protect the personal data (including compliance with the recently introduced Article 74 Medical Devices Ordinance on cybersecurity requirements)

## We are an organization outside Switzerland. Why should we care?

The nDPA has a far-reaching scope of application as it applies to all processing of personal data that has an effect in Switzerland, even if it occurred abroad, for example, the processing of personal data of Swiss citizens by an entity with its seat abroad. Hence, a company that has Swiss employees or conducts clinical trials with Swiss study subjects is likely subject to the nDPA and may even need to appoint a representative in Switzerland.