In May 2018, GDPR (Global Data Protection Regulation) will come into force in Europe. Conventional wisdom is that GDPR will cause significant legal changes for many organizations and result in yet another regulatory-driven upheaval in technology. But is this an accurate assessment of the likely impact?

**Power to the People**

Although some individual rights will be reinforced or extended, the advent of GDPR represents a fundamentally new (and arguably, overdue) approach regarding the ownership and protection of personal data. The main aim is to return control of personal data back to the individual. Furthermore, after May 2018, it will no longer be the responsibility of an individual to prove that personal data was either collected or used without explicit consent. Instead, responsibility will fall upon organizations to demonstrate that consent was sought and received. This change is revolutionary and a reflection of the increased power of regulators after the financial crisis of 2008. The cost to organizations who fail to comply is yet to be seen of course but we expect significant fines to be levied out to non-conformers.

**The Swiss Federal Act on Data Protection**

The Swiss Federal Act on Data Protection (FADP) was first enforced in June 1992 but has been regularly reviewed and amended since, most recently in September 2017 to ensure alignment with GDPR. Despite not being a member country of the EU, (and having no plan to become one) it still makes economic sense for Switzerland to adopt national regulations that are in line with those of Europe, particularly where personal data are concerned. Maintaining similar standards of storage, security and transfer...
are necessary for maintaining the competitiveness of the country, in addition to facilitating easier data exchange with EU countries. Consequently, the most recent review of the FADP was aimed at bringing the Swiss regulation more into line with GDPR, by using identical definitions of personal and sensitive data, adopting the same principles and employing similar terminology. The scope has also been changed to align with GDPR, with an exclusive focus on individuals.

The obligations on organizations defined by the Swiss FADP are very similar to those in GDPR. They will have to prove that:

- Written consent was received from individuals to use and store personal data
- Consent can be removed at any time, and data collected could be corrected/amended
- All personal data are securely stored and protected
- Retention time is minimal regarding the purpose of the collection
- Regular reviews and reports could be produced detailing the individuals on whom data are stored and how data are used.

FADP introduces some limitations on the right to be informed. An individual has the right to be informed regarding how his data are managed, but requests should remain “reasonable” in terms of coverage and of frequency. If getting the information is too complex or too difficult, then the company could partially answer.

FADP also stipulates that organizations must adopt a risk-driven approach assessment and mitigation strategy, similar to that of GDPR.

### Differences between FADP and GDPR

In general, FADP is very similar to GDPR. One area where they differ is data portability. Under GDPR, an individual can ask any organization to retrieve and report all of the personal data for that person in a legible and exportable format. However, this right does not extend to FADP.

One other area of difference is the amount of fines that can be imposed upon organizations for non-compliance. Under GDPR, regulators can impose a fine of up to € 20 million, or 4% of annual worldwide turnover. In contrast, the Swiss regulator may impose a maximum fine of only CHF 250,000.

In addition, GDPR defines the role of a Data Protection Officer who is accorded the authority to levy fines in for non-compliance. There is no equivalent role in FADP. Instead, any compliance breach must be communicated to the local regulatory authority which then assumes responsibility for investigating and levying any fines.

### What will change in Switzerland?

Under previous incarnations of FADP, Swiss organizations were already subject to a number of constraints concerning personal data privacy, including the need to obtain written consent and to report. However, with the closer alignment of FADP to GDPR, Swiss organizations will assume additional duties and responsibilities:

- A duty to inform the individual the reason for collecting their personal data, how the data will be monitored and processed, and how the data will be archived.

The right to be “forgotten”, that is, the right of an individual to demand the deletion of their personal data. FADP will also provide principles and guidelines for dealing with data pertaining to the deceased. Automated decision and profiling are not prohibited but submitted to additional information. Express consent is required for any profiling, and individuals must be fully aware of any automatic decision that should have been taken, as soon as it has a significant impact on them.

Any breach of data security must be reported to the local regulator and to the individuals concerned. All data processing must be documented. Concepts of “Privacy by design” and “Privacy by default” are introduced.
Additional Regulations for the Finance Industry

Client privacy has always been important in the finance industry, especially in Switzerland where "banking secrecy" has long been established and has historically given Swiss banks a competitive advantage. However, that advantage is being eroded as Swiss banks will be forced to comply with the new regulations, including, but not limited to FADP and GDPR.

GDPR required the production of the register of treatments, in addition to what is already required, as for example the Annex 3 (FINMA 2008/7), obligation on banks to guarantee the confidentiality of electronic clients’ data.

Other regulations are also being reviewed, and may further impact the way personal data will be collected, stored, processed, and exchanged. For example, the outsourcing regulation for banks (FINMA 2008/7) and the Swiss Federal law on financial services.

What Should We Do?

May 2018 is approaching. Now is the time to prioritise and plan the activities required in order to be compliant in good time.

We believe that the first priority is to define a clear roadmap to reach GDPR compliance, by conducting an assessment of the gaps and the risks regarding GDPR principles and expectations. In addition to a clear and sustainable roadmap, companies must enhance if needed their breach identification and report process, as well as consents monitoring process.

Tactical solutions, if definitive ones cannot be set up, must be defined to be able to report information requested (ex: register of treatments), and to inform clients.

Finally, as soon as possible, awareness sessions must be provided to all employees within the company, to explain new stakes regarding personal data protection and new behaviors that are requested. A GDPR program could be split into 6 main phases, from defining the governance to the selection of the appropriate IT systems:

Based on our experience with regulatory programs, and GDPR projects in particular, we believe the main challenges to successful implementation will be:

1. Obtaining committed sponsorship from the top management
2. On-boarding all relevant departments into the program including Business, Operations, Legal, Compliance, IT etc.
3. Defining a relevant and feasible Target Operating Model, with appropriate systems and processes.
4. Selecting the most relevant approach to perform compliance assessment (depending on your organization and maturity, the assessment could be done by processes or by GDPR topics)
5. Anticipate the difficulties. From our experiences, following principles are always assessed as challenges: the right to be forgotten, the profiling restriction, the “Privacy by design/default” principle, the necessity to report any breach to regulator within 72 hours, and the necessity to face any client request regarding the use of his personal data.

Conclusions

Because data security and data quality have historically been high priorities for banks, we anticipate that most participants in the industry should be able to accommodate GDPR. However, there will be challenges and they will take time. And now is the time to start tackling these challenges.