KPMG

Boardroom Questions

GDPR/Swiss Data Protection Act
Ready to comply in the new era of data protection?

The General Data Protection Regulation (GDPR) – now fully established in the EU – marks the dawn of a new era in data protection. As Switzerland prepares to follow the EU's lead, what can we take from lessons learned so far? In addition to the deliberate misuse of data, companies were fined in particular for negligence and inadequate cyber security measures. Where do you stand on your compliance journey and what's your strategy for the future of data protection at your organization?

For EU firms and Swiss companies with EU operations, the GDPR compliance process is already well under way. Their task over the coming years is to enhance and refine the rudimentary compliance frameworks they have already set up.

Switzerland is currently in the process of aligning its own Data Protection Act (DPA) to the GDPR and it's only a matter of time before Swiss companies face aequivalent obligations – and challenges – that EU operators did a short time ago.

Regardless of the legal requirements, personal data breaches erode consumer confidence and damage brand and reputation – another reason why boards should put data protection firmly on their agenda.

Now is the time for companies to prioritize compliance and get ahead in data protection.

Why should this topic be on your radar?

- In a world where cyberattacks are a daily event, companies cannot afford to ignore the risk of personal data breaches.
- Offenders with initial – demonstrable – GDPR compliance measures in place are generally treated with greater lenience by the EU enforcement authorities so it's important to document efforts throughout the development stage.
- Switzerland's revised Data Protection Act will mirror the GDPR in terms of compliance framework requirements.
- Boards need to be confident that measures are implemented efficiently and effectively, i.e. that they truly work in practice.
- Compliance testing at an early stage will reveal any gaps. Do measures really hold up in practice to ensure full compliance with all data protection obligations?

What should the board be asking itself?

- Have we implemented the required GDPR compliance measures, and are they effective?
- If GDPR has not been relevant for us as a Swiss company so far, would a GDPR compliance program make sense now in preparation for Switzerland's updated DPA?
- What's our governance strategy in data protection compliance? Have we verified implementation and effectiveness of our compliance framework?
- What's our residual risk exposure?
- Do we communicate our data protection efforts externally in a way that enhances stakeholder trust?

What should the board be asking its management team?

- Which measures still need to be put in place to ensure compliance, safeguard ongoing smooth operation of compliance measures and reduce residual risk?
- What is our plan and budget?
- How efficiently do we operate our compliance framework? Have we adequately considered automation (so called "**e**lectronic **G**overnance, **R**isk and **C**ompliance [eGRC]" tools) and outsourcing opportunities (e.g. DPO Support Services)?
- Who will be responsible for compliance with the new Swiss DPA?
- Is the framework integrated in risk and compliance management and are there auditable controls?
- What are we doing to ensure data protection of any third parties we deal with?

Assess	Design	Implement & Automate	Monitor
Identify your organization's data protection compliance gaps, taking current and future data protection regulations into account.	Design a data protection compliance roadmap specifying the processes, systems and controls that will be put in place to become data protection compliant.	Ensure effective and efficient (eGRC automated frameworks, usage of outsourced DPO services) implementation of compliance measures.	Monitor your organization's data protection compliance on an ongoing basis. Establish controls. Consider using assessments or certification schemes to demonstrate data protection compliance to key stakeholders.

Contact

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich

kpmg.ch/blc

Matthias Bossardt
Partner
Head of Cyber Security
and Technology Risk
+41 58 249 36 98
mbossardt@kpmg.com

Thomas Bolliger
Partner
Information Management
& Compliance
+41 58 249 28 13
tbolliger@kpmg.com