Regulatory updates

Recent regulatory developments

Last update: May 2024

pwc

Contents

1 Other developments 3
1.1 EU General Data Protection Regulation (GDPR) 3
1.2 Revised Federal Act on Data Protection (new FADP) 4

2 International Standards on Auditing (ISA) 6
2.1 ISA 600 (revised) 'Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors)' 6

1 Other developments

1.1 EU General Data Protection Regulation (GDPR)

The GDPR imposes a strict legal framework for data protection and privacy in Europe (and beyond) with regard to the processing of personal data. The Regulation was adopted by the Member States of the EEA.

Status:
- In force since 25 May 2018

Applicability of stricter EU data protection rules

The General Data Protection Regulation (EU-GDPR) has been in force since 25 May 2018. It created a new regulatory framework unifying data protection laws across the 28 European Union (EU) Member States and replaced the previous EU Data Protection Directive.

The EU-GDPR imposes a strict legal framework for data protection and privacy in Europe and beyond with regard to the processing of personal data. With the resolution of the EEA Joint Committee, dated 6 July 2018, the EU-GDPR was integrated in the Agreement on the EEA and, since 20 July 2018, applies to Iceland, Norway and the Principality of Liechtenstein.

Compliance journey

The EU-GDPR comprises rules that require organisations to revisit and refresh their systems and operations for data protection. Collectively, these rules set out a new ‘compliance journey’, which organisations have to follow to comply with the requirements. The EU-GDPR represents a major challenge for many organisations, particularly those with large archives of personal data, multiple links to external firms/data processors and complex IT system landscapes. The implementation of the requirements involves numerous challenges, and it is often very multi-facetted. The regulatory and organisational risks are significant, especially for organisations with business models based on the commercial exploitation of personal data. Serious infringements have already been punished with fines of more than EUR 200 million, while fines of several millions are not uncommon for larger companies. Violations of the regulation are punishable by a fine of up to EUR 20 million or 4% of the annual turnover (which could be global), whichever amount is higher. The EU-GDPR also regulates international data transfers. There is a strict set of rules concerning cross-border data transfers, which requires further analysis. Organisations are responsible for ensuring their cross-border data transfers are appropriately secured. This applies to existing, as well as new transfers of personal data, especially those involving so-called ‘third countries’ (i.e. countries that are not members of the EU or the EEA).

The EU-GDPR’s data protection principles must be respected at all times. The principles of ‘storage limitation’, ‘data minimisation’ or ‘lawfulness, fairness and transparency’ are part of everyday data protection when processing personal data. Additionally, there is a so- called ‘principle of accountability’, which requires companies to demonstrate compliance with the EU-GDPR to the data protection authorities, on the one hand, and to key stakeholders inside and outside of the organisation, on the other hand. The rights of the data subjects must also be respected in a timely manner. In particular, the ‘right to be forgotten’ presents considerable challenges to companies as well as to their sometimes very complex IT landscapes.

As the EU-GDPR represents an important change in data protection law, a careful analysis of further developments is called for even after the two-year transition period and its implementation within organisations. The activities of the supervisory authorities and court rulings on data protection require ongoing and institutionalised monitoring by companies.

Who is impacted?

The EU-GDPR is much wider in its scope than the previous EU Data Protection Directive. Any organisation active in Europe must comply with the EU-GDPR if it processes personal data. This includes those with no establishment in the EU, but which are offering goods and services to people in the EU or are monitoring people in its Member States. For example, a Swiss retailer that has no establishment in the EU but targets its product marketing to customers based in the EU needs to comply with the EU-GDPR. The same applies to businesses which are offering goods and services to people in the EEA or are monitoring people in its Member States.

What can you do?

Since the EU-GDPR has already entered into force, it can be assumed that you have implemented a large part of the new requirements in your company.

We recommend therefore the following next steps:

- Identify the gaps between your current data protection programme and the requirements of the EU-GDPR, taking into consideration your data processors, too;
- Adapt and improve the operational structures to ensure compliance with the requirements, which includes the comprehensive documentation of your data protection processes and the related controls;
- Consider data protection reviews and certification to demonstrate both internally and externally your compliance with data protection rules.

Your PwC data protection expert would be happy to help you increase your level of data protection and ensure your accountability.

1.2 Revised Federal Act on Data Protection (new FADP)

The Swiss data protection legislation is being revised, in particular through the new FADP and the related implementation of Data Protection Ordinance (DPO). The new FADP is modelled on the EU General Data Protection Regulation but has some significant differences.

Status: • Entry into force on 1 September 2023

Revision of the Swiss Federal Act on Data Protection

On 15 September 2017, the Swiss Federal Council published the draft bill of the revision of the Federal Act on Data Protection. The meaning and purpose of this revised bill was to strengthen the protection of personal data and to adapt the existing provisions to the digital age. Moreover, it was intended to adapt Swiss data protection law to the legislation at European level, i.e. the EU General Data Protection Regulation (EU-GDPR). Almost exactly three years after the publication of the first draft, after various divergences and a conciliation committee of the National Council and the Council of States, the bill was adopted by both chambers on 25 September 2020.

One factor that shaped the revision of the new FADP during the three years of consultation was ensuring unrestricted access to the EU's single market. Due to the pressure exerted by the EU Commission in relation to this matter, certain parts of the EU's data protection legislation now appear to have been purposely incorporated into Swiss law. This was done to ensure that Switzerland continues to be recognised by the EU as a third country providing an adequate level of data protection, thus allowing it to benefit from the ability to make cross-border data transfers without the imposition of additional legal safeguards.

Key elements of the bill and differences with EU-GDPR

Like the EU-GDPR, the Swiss bill aims to increase the overall transparency of data processing as well as strengthen the sanctions for data breaches. In fact, it adopts the EU legal terminology in various areas.

It also adopts a risk-based approach, e.g. the data protection duties of the data controller are expanded depending on the privacy risks of the data subjects concerned. Like the EU-GDPR, the revised law requires in principle all data controllers and processors to keep a record of their data processing activities. Moreover, in line with developments in the EU, the new FADP strengthens the role and position of the Federal Data Protection and Information Commissioner (FDPIC).

However, in some areas, the bill differs substantially from EU legislation. For instance, it does not require data controllers to document compliance with the new FADP in accordance with the principle of ‘accountability’. Hence, unlike the EU-GDPR, it does not introduce a 'reversal of proof' approach with regard to data protection. Moreover, specific provisions on the protection of children have not been introduced in the draft bill.

Further differences with the EU-GDPR concern sanctions. The upper limit for fines is CHF 250,000 and is therefore significantly lower than in the EU. Furthermore, according to the new FADP, the employees (natural persons) responsible for violations continue to be subject to criminal prosecution, whereas the EU-GDPR applies sanctions to the entities (companies) responsible.

Consequences of the revision and entry into force

Given that the adoption of the new FADP is a major step in the adaptation of Switzerland’s data protection measures requested by the EU Commission, the risk of the EU finding them to be inadequate is now relatively low. Switzerland should thus continue to be recognised as equivalent by the EU in the field of data protection legislation. This is particularly important for the Swiss economy.

What can you do?

We recommend that companies consider the new FADP, especially if they have not yet taken any measures with regard to the EU-GDPR.

Companies operating in Switzerland need to gain a complete and full understanding of how they process personal data. Following this analysis and applying a risk-based approach, the necessary measures should be taken to ensure that the processing of personal data is compliant with the future law. Your PwC data protection specialist can help you adjust to the new environment.

2 International Standards on Auditing (ISA)

2.1 ISA 600 (revised) 'Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors)'

The standard reinforces and enhances the responsibilities of the group engagement leader for managing and achieving audit quality on the engagement, and the responsibilities of the group auditor for the overall direction and supervision of the group audit and review of the work of component auditors.

Status:
- Effective for audits of financial statements for periods beginning on or after 15 December 2023

The most significant changes made to the standard include:
- The group auditor's responsibility for the group audit along with a change in the definition of the engagement team.
- The group auditor shall determine the components at which audit work will be performed (to this end, the concept of 'significant components' and the 'review of the financial information of the component' as a type of work has been removed) as well as the nature, timing and extent to which component auditors are to be involved.