GDPR essentials and how PwC can help

General Data Protection Regulation – in a nutshell

Stricter EU data protection rules adopted

The General Data Protection Regulation (GDPR) entered into force on 24 May 2016. This creates a new regulatory framework unifying data protection laws across the 28 European Union (EU) member states and replaces the prior EU Data Protection Directive. The GDPR imposes a radical data protection and privacy regulatory framework on Europe and the wider world for the processing of personal data of EU citizens. Although there is a transposition period of 2 years for countries and companies to get ready, there are many new and significantly enhanced requirements that organisations should take action on before the May 2018 deadline.

Are Swiss companies impacted?

The GDPR is much wider in its scope than the previous EU Data Protection Directive and that means that the new law applies directly to more organisations. Any organisations that are active in Europe will need to comply with the GDPR. This includes those organisations with no business facilities in the EU but that are targeting goods and services at people in the EU or are monitoring people there. For example, a Swiss retailer that has no business facilities in the EU but directs the markets products to customers based in the EU will need to comply with the GDPR.

A compliance journey

The GDPR contains a series of new rules that require entities to revisit and refresh their systems and operations for data protection. Collectively, these new rules lay down a new "compliance journey" that entities will have to follow to keep on the right side of the law.

There can be little doubt that the GDPR represents a big issue for many entities and particularly those with large stores of personal data or business models based on the commercial exploitation of personal data. The compliance journey involves innumerable challenges and the task is complex. Entities may find that they have difficult choices to make about their priorities moving forward. Ensuring compliance with the GDPR will require considerable investment in resources and lots of planning.

pwc

The regulatory and litigation risks are considerable and especially so for entities that process sensitive personal data. This comes at a time of a lot of stress in the international transfer environment following recent, high-profile litigation. Entities will need to ensure that global data sharing and transfer models are capable of proving operational adequacy in the event of a challenge.

The GPDR is an important change and one that represents obligations and stresses that must be considered carefully.

Why CISOs should feel concerned

The adoption of the GDPR presents CISOs from many organisations across the globe with numerous new challenges. Key issues to be aware of include:

- Expansion of then definition of 'personal data'
  Under the GDPR, personal data means any information relating to an identified or identifiable natural person ('data subject').

  This definition of personal data is important to information security professionals because it implicates data that may not seem, at first glance, to qualify as personal. IP addresses, application user IDs, Global Positioning System (GPS) data, cookies, media access control (MAC) addresses, unique mobile device identifiers (UDID), and International Mobile Equipment IDs (IMEI) are some examples.

- Establishment of data protection standards
  The GDPR requires organisations to implement technical and organisational measures to ensure an appropriate level of security for personal data they hold. The regulation expressly states that such measures include:
  - The pseudonymisation and encryption of personal data
  - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
  - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
  - A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

- New data breach notification requirements
  The GDPR introduces a name-and-shame mechanism whereby businesses will have to notify the competent data protection authority if there is a security incident that affects the security of the personal data that they hold.

  Notice must be provided without undue delay and, where feasible, not later than 72 hours after having become aware of it. If notification is not made within 72 hours, organisations must provide a reasonable justification for the delay. If the breach is likely to result in discrimination, identity theft or fraud, financial loss, damage to reputation, or other significant economic or social disadvantages for data subjects, organisations will have to notify the breach to the affected data subjects. Importantly, no notification to the data subjects will be required if businesses have implemented appropriate technical and organisational security measures in respect of the data that was affected by the breach. So if, prior to the breach taking place, the data was rendered unintelligible, for example by means of encryption, organisations will not have to notify the data subjects of the breach.

- The high cost of security failures
  The EU wants the new data protection rules to become a board-level issue and it has therefore decided to make the rules subject to hefty fines:
  - If a business fails to comply with its data security obligations under the GDPR, it may get a fine of up to 10'000'000 € or 2% of its total worldwide annual turnover whichever is higher.
  - Still worse, if an organisation is found to be in breach of certain other obligations under the GDPR, the fine may go up to a stunning 4% of its total worldwide annual turnover.

How PwC can help

As a multi-disciplinary practice, we are uniquely placed to help our clients adjust to the new environment. Our data protection team includes lawyers, consultants, cybersecurity specialists, auditors, risk specialists, forensics experts and strategists. Our team is truly global, proposing innovative solutions with on the ground expertise in all the major EU economies. Our range of services includes the following:

- Readiness assessment
  We have developed an interactive risk-weighted survey to cost-effectively assess our clients' GDPR readiness. The survey consists of approximately 60 key questions, with pre-populated answers linked to a maturity matrix. Respondents select maturity ratings across a number of dimensions relating to the compliance framework in place within their organisation and adherence to the data protection principles contained in the GDPR.

  The tool produces a report containing risk statements linked to levels of maturity indicated by the respondents. Risk is assessed by reference to regulatory risk and enforcement trends, consumer and employee satisfaction, litigation risk, and B2B risk relating to third parties and outsourcing.

- Personal data inventory
  The GDPR, along with broader global regulatory and consumer scrutiny, requires companies to make efforts to demonstrate operational adequacy and accountability, rather than simply maintaining compliance. The ability to demonstrate compliance and operational adequacy requires a solid understanding of global data operations. This is possible only through a data discovery and inventory effort and the application of practices to maintain the data inventory over time.

  We have developed customisable and adaptable templates and tools to facilitate the streamlined collection of key data inventory information and to define the data processing efforts across an organisation.

- Comprehensive gap analysis
  We have also established a more comprehensive methodology specifically designed to assess the maturity level of an organisation's data protection capabilities and identify gaps against the GDPR requirements. Our proven, field-tested gap analysis templates include 41 controls grouped into the following eight domains:

  1. Strategy, governance and accountability
  2. Data subject rights and processing
  3. Privacy notice and policy management
  4. Risk management and compliance
  5. Data lifecycle management
  6. Incident response and breach management
  7. Third party risk management
  8. Data protection

  At the end of the assessment, we provide a report including the following insights:

  – A summary of your key capabilities, highlighting the strengths of your data protection capabilities
  – A summary of your key constraints, describing areas of improvements needed to achieve compliance with GDPR (i.e. characteristics of 'industry leading' privacy compared with your status)
  – Your current-state maturity, compared with the risk-weighted GDPR requirements and industry best practices
  – Our recommendations to improve your data protection capabilities and achieve compliance with GDPR
  – Our evaluation of the level of effort required to meet the GDPR requirements.

- Action plan development
  We have a wealth of experience in designing privacy programmes. We can help you design your future-state data protection capabilities by developing a set of pragmatic recommendations, along with the associated action plans and implementation roadmap, to address any identified gaps related to the GDPR requirements. Hence, you will have a clear picture of where you stand, where you need to go and how you can bridge existing gaps.

- Assistance in the implementation of compliance actions
  We have developed strong expertise in advising our clients on compliance strategies, reviews and assurance. We can assist in implementing a broad variety of actions to achieve GDPR compliance, by mobilising our global network of lawyers, IT consultants, and audit and risk specialists. Further, one of the key challenges faced by companies undergoing transformational data protection programmes is managing the complexity, the interdependencies and the sequencing of activities. We have proven experience in monitoring complex programmes and have developed tools and templates specifically designed to help overcome the associated challenges.

Contacts

Reto Häni
Cyber Security Partner and Leader
PwC Digital Services
+41 79 345 01 24
reto.haeni@ch.pwc.com

Nicolas Vernaz
Cyber Data Protection and Regulatory Compliance Leader
PwC Digital Services
+41 79 419 43 30
nicolas.vernaz@ch.pwc.com

Susanne Hofmann-Hafner
Legal Compliance Leader
PwC Tax and Legal Services
+41 58 792 17 12
susanne.hofmann@ch.pwc.com

PwC's global cybersecurity and privacy division