Wake Up Call

RSM

GDPR compliance: You have less than a year to prepare

Have you started your preparations for GDPR compliance? GDPR is applicable to almost every organization worldwide that collects or processes data on European Union (EU) residents, including those not based in Europe and even those without any European operations.

General Data Protection Regulation (GDPR) was ratified to strengthen and unify data protection for all EU residents, whether their data resides in the EU or not and enforcement is scheduled to start on May 2018. The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU that process and hold the personal data of data subjects residing in the EU.

Personal data is any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

GDPR casts a wide net. Entities that interact with EU residents are all subject to this law. Many organizations underestimate the amount of EU data they hold, and therefore may not understand the potential effect of GDPR legislation e.g. EU resident data may be stored in everything from IT systems and portable media devices to spreadsheets and email archives. Companies must examine data privacy protocols for primary (and other) sources of client data.

The new GDPR rules will significantly disrupt how organizations store, manage and process personal data. Substantial financial penalties and reputational damage may be incurred for noncompliance, up to €20M or 4% of an organization's global revenue, whichever is higher.

There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order, not notifying the supervising authority and data subject about a breach or not conducting impact assessment. These rules apply to both controllers and processors, meaning 'clouds' will not be exempted.

Under GDPR, individuals can request that companies provide all data they maintain about them, and extensive, detailed information about how such data is protected. This includes how each customer's consent is secured and tracked on an ongoing basis; the specific purpose for holding this data; and the nature and extent of protections surrounding that data, including any third parties that might be involved. Consumers can also request that all such data be provided to them in an electronic format suitable for porting to a competitor, or that all their data be completely erased from all systems the company uses, including, again, those from any third parties.

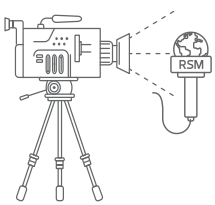
To determine if GDPR affects your organization, you need to ask questions such as:

- Do you offer goods and services to EU residents?
- Do you rely on third parties that store or transmit data to or from the EU?
- Do you collect, transmit or process data pertaining to EU residents?

Keep in mind, it doesn't matter if the services are free.

Organizations should begin identifying or "mapping" EU customer data immediately. It is not uncommon for EU data to reside in different divisions or subsidiaries. This data will need to be protected and segregated from other customer data, much in same way that organizations protect and segregate credit card data through network segmentation standards under the Payment Card Industry Data Security Standard.

Angela Simatupang
angela.simatupang@rsm.id



KEY POINTS

- GDPR may apply even if you don't have operations in the EU
- Timing for compliance is sooner than you think
- Customers can trigger enforcement action
- Start mapping and analyzing your customer data now

RSM Indonesia
Audit | Tax | Consulting

THE POWER OF BEING UNDERSTOOD