KEYRUS
insight into value

EFFECTIVENESS IS THE FORGOTTEN DIMENSION OF GDPR PROJECTS

EXPERT OPINION

Jean-Bernard Guidt, Partner Business & Technology | **Keyrus Management**

Édouard Escoyez, Senior Manager | **Keyrus Belgium**

If companies approach the new European regulations on the protection of personal data solely in terms of compliance, they overlook the one aspect that will actually give them the wherewithal to comply with their obligations over the long term: that is, the effectiveness of the set-ups and systems put in place to secure, control, and report on the use of data.

Introducing, as it does, new obligations for companies as from May 2018, the "GDPR issue" is all too often approached in an administrative manner, as a mere overhaul of the CNIL forms, or as an exercise in implementing organizational and documentary arrangements intended to demonstrate compliance with the regulations. As for some other companies, they wrongly believe that implementing the ISO 27000[1] standards is enough to ensure that their information infrastructure is GDPR-compliant.

Where these approaches go wrong is that they fail to make the connections between the requirements of the GDPR, the obligation to comply with it, and the operational reality of companies. In fact, companies today are entirely dependent on information systems and processes that capture and utilize data – and notably customer data – at all levels of the organization. To take into account only the "compliance" aspect of the GDPR issue is to ignore the crucial question of effectiveness or, even worse, to maintain the idea that anything that is compliant is necessarily effective. This is clearly not the case at all: the first safety belts (without the retractor mechanism) were certainly compliant with the regulations, but they were neither practical nor effective...

THE CHOICES OF ARCHITECTURE DETERMINE EFFECTIVENESS

The challenge is to ensure that the multiple systems using customer data – e-Commerce, Marketing Automation, CRM, the loyalty system, etc. – are effective in protecting personal data against any use that is improper or contrary to the regulations, both in practice, and over time. Since the information system and business processes are bound to evolve, that implies making IT architecture choices based on principles that have proved themselves to be effective. For example:

- Managing the customer repository in a centralized manner makes it possible to have not just a single "point of truth", but also a sole point for controlling the quality of customer data and the use made of them. Doing things this way is much more effective than trying to master these aspects for each individual application that uses or processes customer data.

- Centralizing the management of customer consents/preferences and setting up a single bridge for all applications to access this information allows companies to ensure that all their outgoing communications comply with the most recent version of each customer's consent for each contact channel. In this way, companies not only do away with having to manage and control consents channel by channel, but they also eliminate the inconsistencies, and even the regulatory breaches, that can result from that.

- Segmenting those applications using customer data, according to criteria such as the number of users, level of exposure, sensitivity, etc. makes it possible to create clusters and manage rules no longer at the level of each application, but rather at that of the cluster.

When an architecture is built according to these principles, it enhances the effectiveness of IT teams by making it easier to establish common rules and automate processes for controlling data and their uses. It also helps ensure greater productivity and security for the business teams, as they are protected upstream from risks of data misuse under the GDPR and the company's data policy.

[1]The ISO 27000 group of standards is designed to organize and structure the approach to managing the security of information systems. It does not cover the security architecture.

EFFECTIVENESS IS THE FORGOTTEN DIMENSION OF GDPR PROJECTS

KEYRUS

THE CHALLENGES OF THE "DATA" DIMENSION BEYOND THE GDPR

The applicable regulations, in this case the GDPR, are just one aspect of the management and governance arrangements that need putting in place so as to create value from data – particularly the personal data that have become indispensable for marketing, sales, and the customer relationship. In fact, data is no longer just a resource, but a strategic "asset" to be approached in its entirety. If a company does not have a strategy for valorizing this asset, if it does not have a clear vision of its data-related needs, and if it has not implemented anything to develop its employees' data culture, nor established governance rules ensuring the availability, security, quality, and traceability of data, then it is building its GDPR compliance arrangements on sand, with no foundations or connection with operational reality. On top of this, it will have to renew its efforts with every regulatory development. If, on the contrary, it gets the Legal Department, DPO[2], IS Department, and those departments that use customer data all involved in the GDPR project, then it gives itself the wherewithal to build an organization that minimizes the specific risks linked to personal data, allows those data to be securely used for productive purposes, and is effective as much in meeting external auditing requirements, as in satisfying the data-related needs of the different departments.

[2]Data Protection Officer: representative responsible for data protection, replacing the Data Privacy Officer (Correspondant Informatique et Libertés/CIL). The GDPR makes it compulsory to appoint a DPO in companies undertaking large-scale processing for the regular and systematic monitoring of individuals or sensitive data.

NO ONE TOOL CAN ALONE ENSURE GDPR COMPLIANCE

Regulatory topics always generate a vast amount of communication by solution providers. They all emphasize that their software is GDPR-compliant, whether it be for solutions for managing repositories, transporting information, or reporting. In 80% of cases, these claims are unreasonable, and it is essential to understand that juxtaposing solutions certified as being "GDPR-compliant" in no way guarantees that the organization is compliant overall. On the other hand, certain solutions, designed to match the expectations of the CNIL, do provide real support by enabling companies to supply the audit reports required by the regulations.

From an operational point of view, the GDPR covers so many tools and processes that it is simply unrealistic, whether it be during the phase of establishing compliance, or equally that of maintaining it thereafter, to hope that one single tool can alone address all needs. Identifying which tools are suitable depends fundamentally on the nature of the data, their use within the organization, and the choices of architecture. Companies that embrace all these dimensions will derive value over the long-term from their investment in compliance. In contrast, those that confine themselves to the normative and administrative aspects are undertaking ineffective expenditure that provides no added value and no long-term benefit for the organization.

J-B.G. E.E.

About the authors

Jean-Bernard Guidt

Jean-Bernard Guidt, Sales Manager of Eurobios (2006-2009), then in charge of the Urbanisme & Architecture Competence Center and of the Business & Technology Division of Capgemini (2009-2016), joined **Keyrus Management** in 2017 as Managing Partner. He advises his clients on how to better define their strategy roadmap, the evolution of their operating system and IT infrastructure and to adapt the employees to the organizations. He supports his clients in creating a vision and building a business trajectory.

Édouard Escoyez

Prior to joining **Keyrus** in 2015, Édouard Escoyez worked 16 years for major multinationals. Throughout his career, he has built a wide range of expertise and knowledge defining and delivering analytics solutions in the Banking, Biophrama, FMCG and Chemical sectors. Within **Keyrus**, he is in charge of both Advisory and Implementation in the BI, CPM and Data Governance domains. He is also responsible for the GDPR offer in Belgium & Luxemburg.

About Keyrus Management

Keyrus Management is the Consulting Firm incorporated within the **Keyrus** Group and it combines business know-how with technological expertise in data management.

The complementary nature of these two aspects provides an edge in terms of value, and gives **Keyrus Management** a unique positioning in the consulting landscape.

Keyrus Management helps enterprises of all sizes, whether they be Large Accounts or small- and medium-sized companies, to meet their increased needs for rapid transformation by developing their agility and accelerating Digital use. The firm is developing its activities in France and internationally, supported by the **Keyrus** Group, a specialist in Data and Digital present in some fifteen countries on four continents.

Further information at: www.keyrusmanagement.fr