WAVESTONE

GDPR,
ONE YEAR ON: WHAT HAVE WE LEARNT?

There are now only 8 months left to become GDPR (General Data Protection Regulation) compliant since the program's announcement two years ago in April 2016. What stage of compliance have the relevant major players reached? Will they be compliant by May 2018? What are the most complex projects to date? What can be learnt from the work carried out so far?

Our review is based on a sample of our operations within 20 international accounts (spanning Banking, Insurance, Transport, Energy, Services, Large distribution, etc.) and more than 40 projects

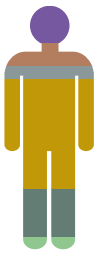
IMPORTANT PROGRAMS ENGAGING THE FULL BREADTH OF COMPANIES' DEPARTMENTS

GDPR compliance programs have a wide-ranging effect on companies, each involving anywhere from dozens to hundreds of stakeholders. Consolidated workload estimates range from 3 to 4 FTEs (full-time equivalents) for smaller and more compliant environments, and up to dozens of FTEs for more complex and less compliant environments.

CONTACT

RAPHAËL BRUN
raphael.brun@wavestone.com
YOURI DUFAU-SANSOT
youri.dufau-sansot@wavestone.com

This workload is generally distributed as follows:



15% for the team in charge of program steering, its coordination and communication/training

10% for the DPO teams, to formalize policies, directives and processes, define the target organization and ensure the compliance of solutions deployed by the business functions and IT teams

5% for the legal team, to interpret the text, propose clauses and legal notices, and arbitrate on legal points identified over the course of the project (namely the proposed retention periods)

45% for the IT and Digital teams, 10% to propose new service offers and IT compliance tools and solutions (in particular, exercising rights, consent, deletion and portability), and 35% to implement changes in existing information systems and to integrate GDPR requirements into the developments-in-progress to achieve compliance

20% for the business teams to map their processes, make them compliant, change the customer journey and improve operating procedures with their partners and employees

5% for the CISO teams and the cybersecurity department to review existing programs of system surveillance, security incidents notification, and rights & access management control to include personal data, whilst helping build the Privacy by Design methodology based on their experience integrating security into projects

Contrary to popular belief, the workload of legal teams and CISOs remains light with respect to the overall burden of GDPR programs.

For most of the organizations we see, the analysis of the GDPR requirements (carried out in the first weeks of the program) is currently either complete or near completion, and has been replaced by more operational projects where there is less of an emphasis on the legal aspect.

As far as cybersecurity projects are concerned, they are less often driven by GDPR programs and more so by existing cybersecurity initiatives.

IT workload should not be underestimated as it amounts to almost half of the total workload for GDPR compliance programs. Although they are not necessarily visible from the start of the program, they are required to operationally implement the changes of business processes, as well as the requirements from Legal and DPO departments.

Some examples

INSURANCE
40+ Business Units
Nearly 300 key stakeholders
Central steering by 4 FTEs

BANK
~ 50 entities
More than 250 key stakeholders
Central steering by 3 FTEs

RETAIL
A dozen de Business Units
Several dozen key stakeholders
Central steering by 3 FTEs

ENERGY
A large regional network
Hundred of key stakeholders
Central steering by 7 FTEs

This distribution of effort will be subject to change in line with the completion of the GDPR program and the beginning of the project implementation phase. Specifically, the workload of DPO teams will increase, with more focus on training, monitoring and project support roles, whilst the effort for IT and Digital teams will shrink once developments are implemented in existing information systems and GDPR requirements are integrated into future developments.

5 AREAS OF GDPR TO INVEST IN...

The implementation of GDPR compliance can be summarized in 5 main aspects:

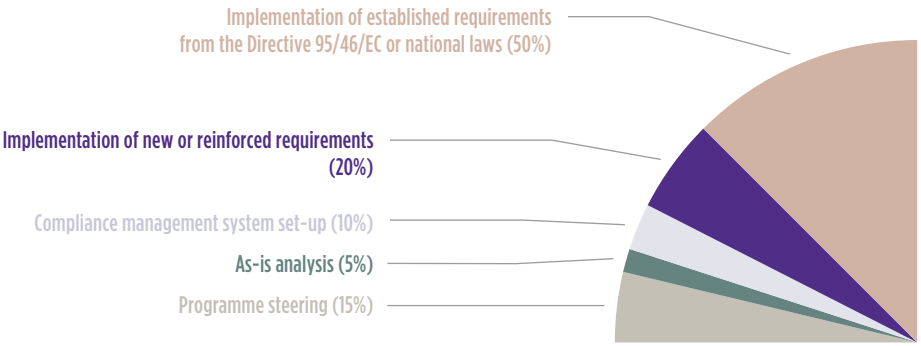
1 **Program steering and expertise** to tackle challenges (15%): project scoping, budget building, action monitoring, reporting, coordination with other projects and initiatives, regulatory watch etc.

2 **As-is analysis** including notably the creation of a record (or register) of processing activities and the identification of main non-compliance areas (5%, mostly business and DPO). Particular attention should be paid to building the register; processing 'to-be-analyzed' should be carefully prioritized to avoid overinvesting in this component of the program.

3 **Compliance management system set-up** including the definition of policies, directives, methodologies and compliance tools, structuring the DPO organization, the establishment of controls and compliance audits, and the training and awareness-raising of involved stakeholders (10%, mostly DPO).

4 **Implementation of new or reinforced requirements** such as consent management, building Privacy by Design support into IT projects, and implementing data portability (20%, mostly business and IT).

Budget breakdown



5 **Implementation of established requirements from the Directive 95/46/EC or national laws** on personal data protection. These include data subject information and rights management (access, deletion…), the ability to retrieve and delete all data associated with a given person within an organization once the defined retention periods have expired, transfer management (to third parties or outside of the EU), improvement of existing security measures, and data anonymization in non-production environments (50%, mostly business and IT).

In the majority of programs, we are working on, roughly half the investments are dedicated to the implementation of compliance actions already required by national or European laws (Directive 95/46/EC) preceding the GDPR.

… WITH 5 COMMONLY NOTICED CHALLENGES…

Once program frameworks are put in place and gap analyses performed, the implementation challenges begin. Whatever the context, the sector of activity, the nature of the data manipulated or the existing compliance level, these 5 topics consistently appear amongst our clients.

The opinion of the regulator on certain topics, the difficulties of interpretation of the text and the lack of maturity of the market. Several GDPR topics, for example the right to portability, still do not have clearly defined implementation guidelines. Pioneering organizations run the risk of wasting resources if they misinterpret a regulation with new or complex requirements, leading to delays in operational implementation. Moreover, for more technical subjects such as data classification and anonymization, many solutions on the market are not yet mature.

The appropriate application of retention periods and the right to be forgotten within existing information systems. The problem is often further complicated due to legacy systems (personal data being used as a unique ID in database systems, fields which are required from a technical point of view but not essential from a business point of view, etc.). These legacy applications can potentially require large investments of approximately €40k to €200k per application. Data deletion requirements are sometimes virtually impossible to implement due to the potential impact on the information system, notwithstanding the difficulties of identifying the data in the first place. This problem can be resolved by data substitution, tokenization or a similar technique.

The management of the business relation with suppliers to ensure end-to-end compliance. For example, the collection, inventory and revision of supplier contracts can be significant depending on the degree of decentralization of contract management. The integration of GDPR clauses into future contracts should be the main focus, as this is the most efficient approach moving forward. For existing contracts, expectations should be communicated to suppliers by reminding them of the obligation to include GDPR requirements. Do not portray this as a contractual engagement which needs to be renegotiated. The effective application of contracts should also be considered as a point of attention, which may require the application of supplier controls or even auditing.

The implementation of project support methodologies (Privacy by Design) and privacy risk analysis tools (such as Privacy Impact Assessments) that are realistic in terms of constraints and budget, and which project leaders can easily learn independently. Even if certain organizations have already introduced processes to integrate security into projects, these need to be redesigned and the relevant stakeholders need to be trained. Best practices include prioritizing simplicity and pragmatism over completeness, and focusing on the most sensitive projects first.

Identifying expert resources that can join the DPO team or contribute to various topics. These resources are extremely rare and difficult to find, whether internally or from external service providers, consulting companies or law firms. Therefore, it is important to effectively distribute tasks and avoid trying to position one expert in each aspect and role of the program. The program directors can come from the IT department, lawyers can be quickly educated on privacy issues, and internal control teams can help the relevant processes evolve. These environments can be heavily burdened with client regulation, so integrating initiatives that consolidate work and increase deliverable production can increase efficiency and convenience. Considering the challenges and the scale of the program, rigorous and pragmatic steering is essential. This can be temporarily allocated to a specific team, independent of the future DPO organization.

The DPO position can attract both positive and negative feedback from business, depending on the context. Whereas existing compliance teams may be enthusiastic about assuming this task, other teams may not be willing to take on this role as it can be perceived as burdensome, constricting, or overly negative.

… AND CONSTANTLY GROWING BUDGETS

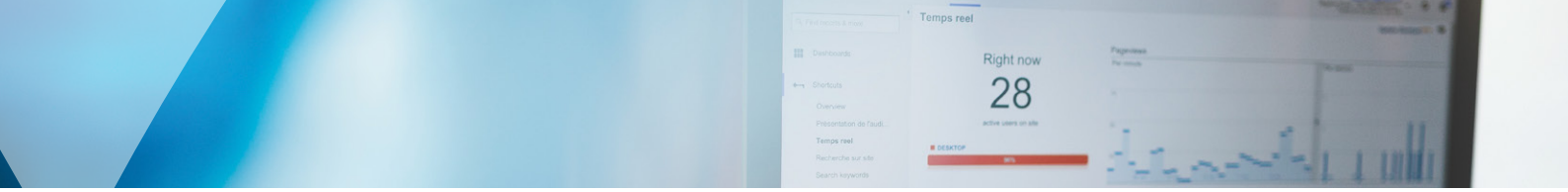
GDPR is a new concern. Securing your private life is not. The UK's Data Protection Act, for example, has existed since 1984; such historical legislation has led to a false assumption that all organizations have had a high level of compliance, thus reducing the concern related to sanctions.

> "GDPR programs have taken significant time to implement, and with limited budgets. The progress of as-is assessments, gap analyses and the complexity of measures to be implemented often lead our clients to regularly and significantly increase their budgets."

For most large international accounts, GDPR programs have taken significant time to implement: most front-runners started at the end of 2016, and for numerous programs, a more realistic launch time was the first quarter of 2017. Similar to other projects of this scale, the progress of GDPR programs has been inhibited by the complexity in role and responsibility allocation, between resource limitations in corporate departments, and the delays associated with local entities waiting for specific direction from the group before implementing compliance projects.

Though most GDPR programs began with limited budgets, the progress of as-is assessments, gap analyses and the complexity of measures to be implemented often lead our clients to regularly and significantly increase their budgets.

GDPR programs have currently been implemented by a range of large international groups. For organizations working with a reasonable amount of personal data and limited Big Data or profiling activities (mainly



B2B), budgets range from 1-5 million Euros. For companies with several business functions and numerous entities/subsidiaries (generally B2C), the budget can reach 20-50 million Euros. For major international players, notably banks or insurance leaders, their initial budgets have reached several hundred million euros, which are now being optimized and prioritized. The wide-ranging changes to be implemented across multiple applications are another factor that is rapidly increasing the costs.

Management boards are increasingly expecting business lines and IT departments to de-prioritize other budgets or are relying on existing programs (notably cybersecurity, contracts review, data archiving or customer relationship programs) to absorb projects which have been identified.

> "May 2018 is no longer the final compliance deadline, but is the end of the first stage of achieving compliance"

The considerable financial impacts of such programs, as well as the corresponding budgets of deployment, now require a review of initial planning (May 2018) so that budgets and workloads can be evenly distributed over time. May 2018 is no longer the final compliance deadline, but is the end of the first stage of achieving compliance; the most important work and a clear roadmap outlining the next steps have yet to be completed.

HOW TO EFFECTIVELY EMBARK ON THE ROAD TO COMPLIANCE BETWEEN NOW AND MAY 2018:

In our opinion, simple rules can be followed to set your organization on the path to compliance:

Smart steering. Create a steering structure at group level which does not solely aim to enforce and control, but primarily ensures it can propose operational tools to help entities enforce compliance. Additionally, the steering structure must produce these tools quickly enough such that local initiatives are not inhibited. For example: do not wait for the end of 2017 to propose a PIA method.

Identify and prioritize high-risk processes: certain cases are easy to identify (e.g. processing health data, fraud prevention) whilst others require subject matter expertise (SME). For example, human resource (HR) folders on "internal law" are, in theory, anonymized. However, in practice they are only replaced by a pseudonym, and therefore are often easily re-identifiable.

Do not attempt to analyze all processes by May 2018. Analyzing all processes takes significantly more time than building a register (at least 4-5 times as much). This analysis, which requires specific experience and expertise in data privacy, cannot be carried out exhaustively by 2018 (due to cost constraints and a lack of capable resources). It is therefore better to prioritize the high-risk processes (20-30% of processes) and establish a clear roadmap to analyze the rest.

Address topics simultaneously to be more agile. The program does not need to have a top-down approach where operational staff must wait for tools and group politics for several months before being able to start their compliance work. All stakeholders involved (business lines, compliance, IT, Legal, etc.) should be able to progress in parallel, and support each other with a flexible and agile approach. For example, IT teams should not wait for business lines to identify retention periods and to require implementing them within information systems. Instead, they should focus on identifying applicable solutions and associated tools (for example, irreversible tokenization).

Pool as many things as possible. Reinventing the wheel will not do anything. Corporate teams can propose and generate a toolbox of time-savers. Instead of asking all entities to build their register, it would be more useful to propose a template consolidating 70-80% of processes common to all entities. The program will therefore be simplified and the burden of compliance will be significantly reduced.

Explain, explain and re-explain: GDPR and its implementation is a complex subject requiring the attention of numerous stakeholders who are new to this topic. It is therefore essential to educate by closely supporting the project leading teams to help them understand expectations, take ownership of the issue and ensure they fully engage in the definition and implementation of solutions.

Make compliance an asset for your brand. GDPR programs are commonly seen as a constraint by operational staff. However, the protection of privacy is a major concern for everyone, both clients and employees (here is our previous paper on privacy in a digital world, which includes exclusive insights on peoples' perception of privacy in 6 countries: https://www.wavestone.com/en/insight/privacy-digital-world-compliance-trust/). It is therefore essential to integrate this program at the heart of data initiatives and associated agreements. Any communication surrounding the program should highlight transparent and compliant personal data management as a marketing asset in customer relations, as well as a positive image driver for the employer brand and the employee relationship.

WHAT CAN BE TAKEN FROM THIS PAST YEAR?

GDPR programs have been slow to get started. As a result, there has been reduced awareness of the regulation's impact, scale of the programs and required budget.

Nevertheless, since the beginning of 2017, numerous programs have entered into the remediation phase and the first solutions have begun to emerge. However, not all projects can be completed by May 2018, even though key actions have been taken and high risks mitigated.

In addition to deploying as many actions as possible by May 2018, our clients are organizing themselves to rapidly establish an operational DPO function. Their goal will be to leverage sufficient budgets to drive forward all identified actions while implementing long-term processes, thus guaranteeing compliance over time.

WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France). The firm is counted amongst the lead players in European independent consulting.

Wavestone's mission is to enlighten and guide their clients in their most critical decisions, drawing on functional, sectoral and technological expertise.