Deloitte.

The time is now

The Deloitte General Data Protection Regulation Benchmarking Survey

How are organizations facing the challenge of complying with the most radical overhaul of data protection laws in a generation?

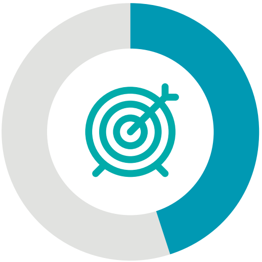
Contents

Understanding the challenge

Deloitte has conducted a General Data Protection Regulation (GDPR) benchmarking survey across a sample of organizations and industry sectors in EMEA. The aim of this survey was to understand how organizations are preparing for GDPR compliance, how advanced their implementation plans are, and how confident they are of achieving their goals by 25 May 2018.

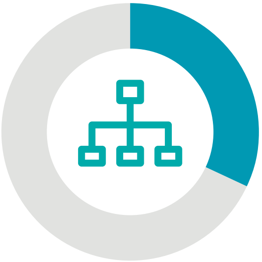
The results of the survey indicate that organizations are taking a wide range of readiness approaches, driven by the combination of the potential for significant fines, the increased obligation to demonstrate proactive compliance and the complexity and ambiguity of some of the requirements.

The results show that approaches to compliance and remedial spending vary widely; 39% of organizations report spending less than €100,000, whilst 15% report spending more than €5 million. There is no correlation between organization size (by headcount or revenue) and spend, nor any clear trends in different industry segments. Our results reported examples of organizations with fewer than 10,000 employees spending over €2.5 million, but other examples of organizations with more than 50,000 employees spending less than €250,000. Similarly, there is a large variation in privacy headcount: 45% of respondents have a dedicated privacy function, 32% manage privacy within another function, and 23% have no formal privacy function.



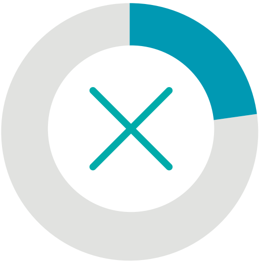
45%

dedicated privacy function



32%

manage privacy within another function



23%

no formal privacy function

There is little correlation between organization size (by headcount or revenue) and spend, nor any clear trends in different industry segments.

These results may be explained by a number of different factors:

- Significant historical variance in approaches to the current regulations means that organizations have varying starting points in regards to their privacy maturity.
- Many organizations are struggling to define tangible outcomes that they want to achieve by May 2018, leading to a lack of ownership, no defined target state, and inconsistency in many programs.
- The momentum generated by the potential for significant fines is tempered by the general uncertainty over the extent to which they will be used, leading to the most common question: *What is good enough?*

Overall, only 15% of organizations surveyed expect to be fully compliant by May 2018, with the majority instead targeting a risk-based, defensible position. The main reasons given are the lack of time left to achieve compliance, the ambiguity of the text of the GDPR and the difficulty of fulfilling some of the requirements.

1

Time left to achieve compliance

2

Ambiguity of the GDPR text

3

The difficulty of fulfilling some requirements

This report examines these matters and makes pragmatic recommendations on how to comply with the areas respondents feel present the greatest challenges. Most importantly, this report considers how privacy can become more than a compliance exercise; how it can become a real business asset and enabler, and maybe even a competitive advantage.

Privacy as an enabler

Beyond highlighting the greatest challenges and concerns regarding GDPR requirements, the results highlighted another trend: privacy as an enabler. 61% of respondents see further benefits of remediation activities beyond just compliance. And of those, 21% expect *significant benefits*, including competitive advantage, improved reputation and business enablement.

By way of example, records of data processing can support other areas of GDPR compliance, such as the management of data subject rights and risk assessments, but can also assist with wider business enablement. Adopting an innovative approach to the *records of processing* requirement has additional business and privacy advantages such as the identification of system redundancy or superfluous suppliers. Having a detailed inventory that helps identify the roles of systems and processes will support the identification of any duplicated efforts and, where something can be decommissioned, facilitate cost saving activities. This is an opportunity for privacy to provide a concrete and tangible return on investment.

Increased transparency requirements offer another excellent opportunity to engage with customers to demonstrate the measures the organization is taking to protect their data. As well as ticking a compliance box, with the right engagement strategy the exercise can demonstrate data ethics, build trust with customers, and increase the consumer trust in the brand.

These examples demonstrate how organizations should take advantage of the opportunity to use privacy to strengthen their businesses. The use of innovative approaches to compliance requirements can help organizations to understand the privacy impact on wider business risks and pain points, and to gain better insight into peer activity to maximize the role of privacy in the organization's strategy.

The key here is intelligent implementation, capitalizing on the need for change and transformation to make a compliance requirement a real business enabler. Organizations should focus their efforts not just on *what* needs to be done, but on *how* it can best deliver real long-term benefit.

61%

of respondents see further benefits of remediation activities beyond compliance, supporting Deloitte's view that the GDPR offers the ideal opportunity to view privacy as a business enabler

Time left to achieve compliance

ONLY 15% ☑

expect to be fully compliant

Most organizations do not feel they have time to implement the necessary activities to achieve compliance before the effective date of the Regulation, i.e., 25 May 2018. Only 15% expect to be fully compliant by then, with 62% instead opting for a risk-based, defensible position. The remaining 23% have even lower expectations for their compliance position.

62%

opt for a defensible position

Despite a two-year period in which to prepare, the findings support a pattern of slow movement from organizations: 33% have not yet determined what increase in headcount will be required to manage business as usual privacy compliance under the GDPR; 45% have not identified legal bases for processing; and only 38% of data controllers expect to have reviewed all processing contracts by the effective date.

Further, although 89% of organizations have, or plan to have, a formal GDPR readiness program, only 45% had completed a GDPR readiness assessment. Most of these programs are led by Compliance (39%) and Legal (31%) departments.

But beyond the statistical data, written answers from survey respondents suggest that the ambiguity of the Regulation's text and the significance and complexity of its requirements, has left many organizations choosing to mitigate their risk exposure rather than strive for full compliance.

Although 89% of organizations have, or plan to have, a formal GDPR readiness program, only 45% had completed a GDPR readiness assessment.

Deloitte insights
GDPR programs should not be seen as a race to get over the line by 25 May 2018. While there will no doubt be some fanfare and publicity around this date, organizations should be defining their target state for both this date and the longer term. Key considerations must be around building a sustainable approach to privacy compliance, and a robust operating model to support it.

Regulatory ambiguity and a lack of guidance

The scope of the GDPR – covering organizations of all sizes and sectors that process personal data – leaves regulatory bodies with the difficult task of providing meaningful guidance that is individually relevant to such a wide audience. Respondents repeatedly raised the challenge of interpreting the Regulation text as a key issue, and welcomed further guidance from the Article 29 Working Party (WP29).

Many organizations have therefore been left struggling to answer the question *How far is good enough?* when determining what to do.

54% of respondents noted that the potential for fines of up to 4% of global turnover made them pay more attention to the Regulation. This could suggest that some of the remaining 46% of organizations remain sceptical that supervisory authorities will levy the full extent of their enhanced monetary penalties, but nonetheless feel it is important to address the requirements.

54% of respondents noted that the potential for large fines under the GDPR made a difference to their approach

The ambiguity of the Regulation’s text, and the slow publication of guidance from regulatory bodies is a key concern for respondents.

Deloitte insights
Guidance from the WP29 will never meet all organizations’ needs; many approaches will depend on the exact context of the business processing. Organizations should focus on making progress where there is certainty in the requirements, and, where there is still some debate, accelerate the foundational steps that will be required regardless of the final regulatory position or guidance.

The challenge of compliance

The GDPR contains a wide-ranging set of requirements that span different business responsibilities, including some that exist under the current legislation, and others that present entirely new challenges.

The technology neutral text of the Regulation may set out the *what*, but it is clear that organizations are continuing to grapple with the *how* of implementation. As a consensus on best practice develops, and regulatory positions are clarified, this problem will be alleviated with time, but in the short term will continue to test organizations.

Our survey showed that the following requirements present the greatest challenges to organizations, in order of difficulty:

1 **Consent – ensuring consent is informed, unambiguous and recorded**

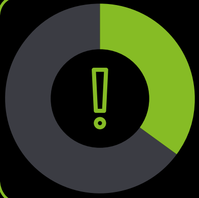
2 **Right to erasure – managing and facilitating data subjects' right to request the deletion of personal data**

3 **Records of processing activities – developing and maintaining a register of personal data processing**

4 **Accountability – keeping records of decisions and positions, and demonstrating compliance**

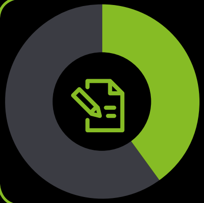
5 **Data portability – providing the ability to port personal data from one data controller to another in certain circumstances**

Other requirements were perceived by respondents as *simpler to implement*, and *quicker wins*, such as:



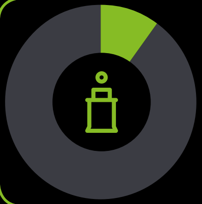
35% of respondents have a data breach reporting procedure that is aligned to GDPR requirements

Breach notification:
35% have a data breach reporting procedure that is aligned to GDPR requirements, with 62% planning to have this in place by the effective date. 41% are *confident* or *very confident* that they will be able to report within 72 hours. 42% are *somewhat confident*, and 17% are *not confident* that they will be able to do so.



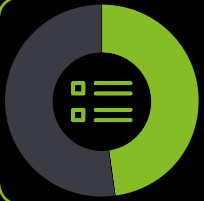
40% of respondents have begun identifying and updating privacy notices

Transparency:
40% have begun identifying and updating customer privacy notices.



10% of respondents expect their DPOs to sit on the board

The appointment of Data Protection Officers:
10% expect their DPOs to sit on the board, with 42% sitting one layer down. Most DPOs will report into compliance (25%) or legal (29%).



48% of respondents already have a PIA procedure in place

Privacy Impact Assessments (PIAs) were also notable for their progress:
48% of respondents already have a PIA procedure in place, although 44% of those need to update their procedures to align with the GDPR.

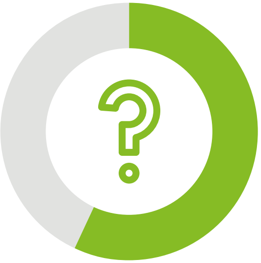
Deloitte insights
Organizations are faced with complex questions in many areas of the GPDR. There will often be multiple ways to appropriately meet the requirements. However, organizations need first to assess the options open to them and perform a cost-benefit analysis. Fundamentally, the target state should be driven by risk appetite and how they view privacy – as a regulatory requirement, a business enabler, or perhaps even a way to gain a competitive edge.

Consent

Consent is one requirement that may have a very direct impact on how organizations interact with their customers and, particularly in the case of direct marketing, the changes could have a real commercial impact.

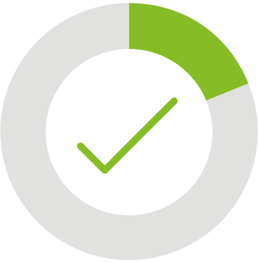
Only 10% of respondents believe their current consents are adequate and 57% of respondents have yet to decide how to ensure their consent mechanisms meet the new, higher standards of consent mandated by the GDPR. 19% have not yet determined how to maintain records to demonstrate valid consent. Only 17% of respondents plan to introduce a new solution to manage consent.

Supervisory guidance published on consent, such as that of the UK's Information Commissioner's Office, notes that a refresh of all existing consents will be necessary if they do not match the GDPR standard, or if they are not properly documented to provide proof of consent. In practice, this means that organizations may face the task of managing a significant re-consenting exercise. It is clear to see why many would view this as unattractive; the exercise carries the risk that individuals will not provide new consent, impacting organizations' ability to market to them. Unsurprisingly, only 19% of respondents plan to undertake a re-consenting exercise.



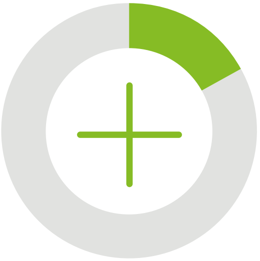
57%

of respondents have yet to decide how to ensure their consent mechanisms are compliant with the GDPR



19%

of respondents plan to undertake a re-consenting exercise



17%

of respondents plan to introduce a new solution to manage consent

Some organizations advocate the use of unambiguous consent, arguing that privacy should not only be regarded as a business enabler but also a business winner. Unambiguous consent mechanisms, combined with succinct and clear privacy notices, can show an increasingly privacy-conscious public that their personal data is being handled appropriately, and that their privacy is taken seriously.

A re-consenting exercise may be required in instances where current consent gathering does not meet the higher standards of the GDPR.

Organizations should consider if another legal basis, such as legitimate interests, could be used to justify the processing of personal data instead.

Deloitte insights

In light of the increased stringency of processing based on consent, organizations should consider whether they can use the *balance of legitimate interest* as the legal basis to justify the processing of personal data. It will likely depend on how intrusive their profiling and direct marketing is, but may offer a simpler and more pragmatic solution. However, organizations should recognize that the legal basis for processing personal data cannot be retroactively applied, and notices may still have to be supplied.

Where a re-consenting exercise is necessary, organizations should look further than just an opt-in tick box. The benefits of opting in really should be made clear, and the use of creative, interactive methods should be considered for the obtaining of unambiguous consent.

Organizations should also be tracking the revised ePrivacy Regulation, which may have an impact on where consent must be used for profiling.

Right to erasure and to data portability

A key challenge that organizations face when determining their approach to individuals' rights under the GDPR, is estimating the extent to which individuals will exercise their rights. Without a clear approach, it is difficult to determine how to prepare for this. Will you get a handful of requests a year, or the nightmare scenario of 10,000 requests for data to be deleted on day one?

64% of respondents have yet to prepare estimates on how many requests for erasure they are likely to receive, which highlights the difficulty in predicting how individuals will use this right.

The right to data portability was deemed less of a challenge than erasure, despite the fact that data portability is a new requirement under GDPR, whereas the right to erasure is an evolution of what exists currently. Notably, the right to erasure now requires controllers who have made data publically available to take *reasonable steps* to inform other controllers of the request for erasure.

59% of respondents have yet to prepare estimates on how many requests for data portability they are likely to receive, and 21% have no plans in place to address the requirement. 26% expect to respond on an ad hoc basis with no specific process, with 42% using manual processes, and the remaining 11% using an interface to automate responses to requests.

Finding all data relating to an individual and deleting it can be performed manually, but organizations need to consider the feasibility of doing so should they forecast a significant volume of requests. The results indicate that 96% of respondents have, or are, investigating the use of tools to help with GDPR compliance, with many considering data discovery, data inventory, and data flow mapping tools, all of which can assist with erasure requests.

64%

of respondents are yet to prepare estimations on how many requests for erasure they are likely to receive

59%

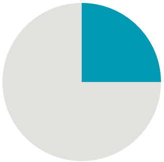
of respondents have yet to prepare estimates on how many requests for data portability they are likely to receive

Deloitte insights

When designing an approach to meet individuals' rights, organizations should consider the likelihood and impact of different volumes of requests being received. Alongside this, there should be consideration of the different options, ranging from a manual, reactive approach through to some level of automation. Each can provide a suitable solution, but will have different cost implications – whether upfront investment is required, or an increase in manpower to deal reactively with requests.

Records of data processing

A quarter of respondents have yet to decide how to approach compliance with Article 30, but the majority (57%) plan to undertake a manual data discovery exercise



It is not surprising to find that the new requirement to maintain a record of processing is reported to be one of the most challenging, and nor is it surprising to see that organizations are approaching it through a range of methods with no clear preferred option. 25% are still undecided on how to approach compliance with this obligation, while the majority (57%) of respondents are planning a manual data discovery exercise. 11% will use tools to comply, and the remainder plan other approaches.

Article 30 lends itself well to the use of tooling. Data flow mapping and data inventory tools, both of which would provide support to meeting Article 30, are popular among respondents, with 40% *definitely considering* tools to enable data flow mapping. This indicates that tools will play a significant role in this area of compliance in the future, and organizations can expect use in these specific technologies specifically to grow.

Intelligent and innovative use of records of data processing not only offers the opportunity to address a significant GDPR requirement, but also offers the opportunity to develop a repository of data with a wider business benefit.

As well as being a key compliance responsibility, handled correctly, this requirement can support other areas of GDPR compliance, such as the management of data subject rights, accountability and data quality.

40%

of respondents are considering tools that will enable data flow mapping

Deloitte insights
Building an inventory of personal data, or data flow mapping, should not just be seen as necessary for meeting the requirements under Article 30. On its own, Article 30 could be met in a very simple way, but understanding what personal data you process is also key to demonstrating accountability, so it should not be addressed in isolation. It will be important to have an appropriate operating model setting out roles and responsibilities to ensure that inventories are kept up to date.

Top five thematic considerations for implementing a GDPR program

Top five thematic considerations for implement

1 Executive sponsorship, business accountability and multi-disciplinary approach

Senior visibility and sponsorship is key. GDPR touches all aspects of an organization's operations and you need the right support to drive change.

This is not just a Legal or IT problem. Business, system and data owners all need to be made accountable for how they handle personal data for the required change to be embedded.

A wide range of stakeholder engagement is required. There are few compliance topics that have implications across such a wide range of areas, including customer engagement, marketing, security, personnel management and technology.

2 Target state definition and outcome-based approach

In many programs we see a vacuum between the program team and the business, with each side looking to the other for increased guidance or more ownership. A clear, tangible and agreed target state across each GDPR area is required to bridge this gap.

It is important to drive towards collective outcomes; this may mean in some cases that the program team lets the business decide how to implement certain requirements, albeit within given parameters. It is equally important to determine where there has to be absolute consistency, for example, with consent and marketing.

ing a GDPR program

3 Risk appetite and risk-based approach

The Regulation encourages a risk-based approach. This can be applied across many aspects; from completeness of your data inventory, to which systems you proactively analyze and prepare so they can deal with rights, such as portability and erasure.

Initially, setting out the risk appetite is a difficult but important task. Is your goal just compliance, or for privacy to be a strategic initiative?

Set tangible parameters, for example, the program will cover 50% of key systems that in turn addresses 90% of your most high risk personal data.

4 Targeted internal messaging – see the benefits

The GDPR may be well down the priority list for many people you engage with and whose support you need. It is vital to ensure internal messaging is relevant such that everyone can see the importance of the topic. This involves understanding their individual role, the impact of getting it wrong, and the benefits that a proactive approach to privacy can bring in terms of customer trust and engagement.

5 Operating model – think long term

This is not something that is going away anytime soon. Make sure your program includes the definition of a long-term operating model that sets out roles and responsibilities such as how privacy risk is managed and how it is monitored and assessed.

This should include the role of enabling technology as the program matures; where efficiencies can be gained rather than knee-jerk technology purchases.

Contacts

Annika Sponselee
Partner, Deloitte Netherlands
asponselee@deloitte.nl

Erik Luysterborg
Partner, Deloitte Belgium
eluysterborg@deloitte.com

Peter Gooch
Partner, Deloitte United Kingdom
pgooch@deloitte.co.uk

Visit us on our website for more information:
www.deloitte.com/GDPR

Deloitte.