IDC's GDPR Readiness Assessment & Recommendations

THE GDPR DEADLINE IS ALMOST HERE HOW READY ARE YOU?

Sponsored by Symantec

Introduction

Thank you for taking part in IDC's GDPR readiness assessment survey. This study enables you to quickly assess your organisation's readiness, based on IDC's in-depth understanding of the GDPR requirement and the roadmap to compliance. Although the requirements of GDPR are many and various, there are some primary indicators that reveal the state of readiness in organizations, and it is these indicators that we use to determine readiness. This report provides you with essential guidance in the development of your security strategy, and includes recommendations on how to progress your organisation toward a compliant and sustainable position in preparation for May 2018.

What GDPR means for your organisation

The EU General Data Protection Regulation (GDPR) is now in force with a transition period until 25th May 2018. IDC research shows that many organisations still appear to have little or no understanding of the regulation, its scope, timeline or impact, despite the risk of huge penalties of up to 4% of global turnover, as well as potential lawsuits, suspension of personal data processing and damage to reputation. Others are more advanced, but are struggling to prioritise activities until May 2018, and to understand how to operationalise compliance after the deadline.

GDPR compliance is required by any organization – regardless of their location – that processes the personal data of "data subjects" (the natural person to which the data relates) in the EU. Processing of personal data refers to what can be done with data i.e. data activities such as: requesting, collecting, storing, searching, forwarding, deleting etc. The definition of processing is very broad: it is best to think of any action that 'touches' personal data as being in scope. GDPR also mandates the consideration of personal data at the time of the inception of a business process or product design, under the requirement for Data Protection by Design and by Default. This embeds data protection in the heart of an organization's innovation process.

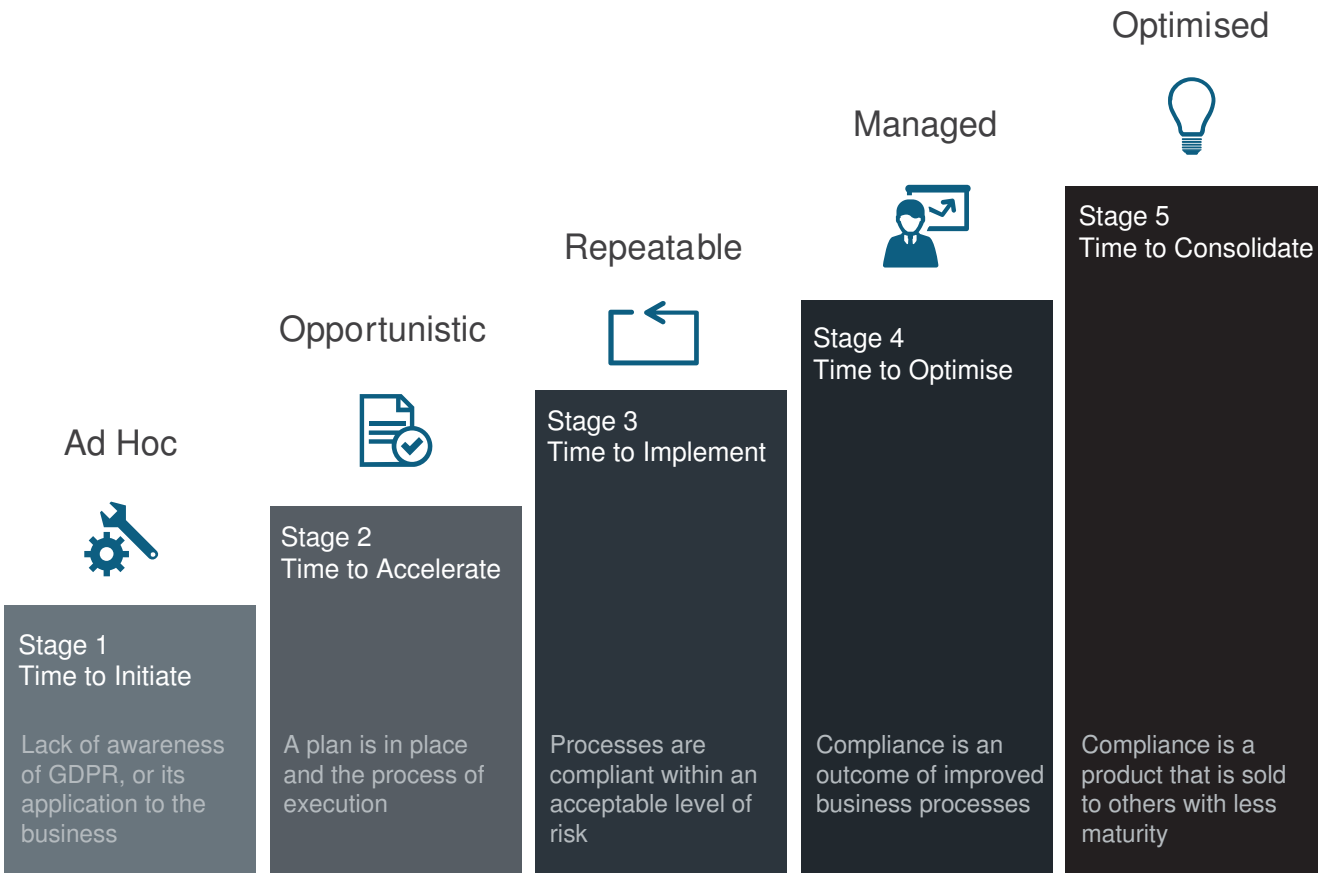
GDPR therefore changes the way in which organisation's do business. In many respects that is the point of GDPR. Arguably, GDPR – in principle – is little different from existing legislation. But the consequences of getting data protection wrong increase substantially, where sanctions are designed to be "dissuasive". That is, GDPR wants organisations to take data protection more seriously than they do at present.

Taking stock of where you are in your compliance programme is apt: at worst it confirms that you are on track with your planned compliance activities. But it may also act as a reality check, both against your aspiration and against your peers. Use this assessment tool while you still have time: the clock is ticking and the requirements are wide reaching. Good luck.

IDC's GDPR Readiness Assessment & Recommendations

Your overall GDPR Readiness Assessment Result

IDC sees five stages to GDPR readiness, with organizations just starting out at Stage 1, and those that are achieving compliance at Stage 5. Based on your answers to this assessment, your organization is at **Stage 1: Time to Initiate**.



In addition, we have ranked you out of five stages in each of the following three individual areas of GDPR so that you can get a good idea of where you need to focus your attention most keenly. These areas are:

- Overall GDPR Approach, Aspiration & Leadership
- Data Awareness
- Risk Awareness, Assessment & Mitigation

Overall GDPR Approach, Aspiration & Leadership

GDPR is more than just about IT security – it involves how the business approaches the concept and culture of data privacy. In order to achieve success, you will need to have the buy in and support of the business, from top management down to individual business units. Fostering a culture of joint responsibility is key to achieving long term sustainable compliance.

STAGE 4: Time to Optimise

Your well on your way, but don't think of stopping just yet. organizations that fall into this category of managed readiness have a firm appreciation of the regulation, its scope, compliance requirements and potential penalties. They have begun to put measures in place to comply but need to step up their activities to meet the May 2018 deadline.

Companies in this stage may have a plan for overall compliance but this may come at the expense of operation efficiency. That’s fine: there is an expediency dimension to GDPR compliance. But after compliance comes optimisation: embed your compliance processes in business as usual. This is tougher than it sounds, so start thinking now about what this might look like for your organization.

By your own admission, you have high aspirations for compliance with GDPR. This should put you in a strong position should a regulator take interest in your activities. Make sure you can evidence your efforts, as this is a crucial part of compliance. The driver for your compliance activities maybe internal efficiency, or improved information given. Or it may be to seek competitive differentiation, possibly through best practices. Whatever your motivation, it is driving you towards being a leader in GDPR compliance. The focus should remain on completing your compliance activities by May 2018, but on the horizon should be an understanding that your compliance processes may not be optimised for operational efficiency. Baking GDPR compliance into business as usual is a step beyond straightforward compliance, but this is where the real benefits lie.

Your score is boosted substantially by the presence of a cross functional compliance task force or governance board that spans multiple stakeholders in your organization. The engagement of all relevant stakeholders is a critical success factor in any GDPR program, and the existence of such a coordinated approach significantly increases the ultimate success of any compliance activity. The other major critical success factor to consider now is the leadership of the GDPR program. It matters less where this leadership stems from, and more that the leader has the authority, knowledge and charisma to lead a strategically important program of activities.

Data Awareness

Information governance is the underlying discipline that enables compliance with GDPR. Bringing all personal data into the scope of your information governance function is mandatory. You need to know what personal data you have (accounting for the very broad definition used by GDPR), and also its location, consent, lifetime, and so on. Demonstrating to regulator that you have a good handle on personal data is the first step in compliance.

STAGE 4: Time to Optimise

You are in the advanced stages of information governance and you have high confidence that you like you can locate all instances of personal data in your organization. You also have a good understanding of both structured and unstructured data, and are likely to be able to service the new rights of access, rectification, erasure and portability.

You are in the tiny minority of organizations that are completely confident in their ability to identify and locate all instances of personal data in their organizations. Well done. But make sure that staff are not creating copies of data – probably for good reasons – that are out of compliance. Data copies are made frequently, for reporting, analysis, back-up and so on. Make sure you have the processes in place to avoid this happening in future.

You are very data aware. Good: a prerequisite for GDPR compliance is knowing what data you have, where it is, and why you have it. You need this in order to compile a record of data processing, mandated under Article 30. You will also avoid a breach of the principles of purpose limitation, data minimisation and storage limitation.

What now? Focus on the gaps in your knowledge of data and its location. Understanding the reasons why you have the data (purpose limitation) is also important, and you need to understand where different regulations apply to different classes of data (such as special categories and data relating to children).

Above all, remember that regulators will tolerate breaches and minor non-compliances. But they will not tolerate a lack of evidenced effort. It is insufficient to be data aware: you must be able to demonstrate data awareness.

Risk Awareness, Assessment & Mitigation

GDPR is all about risk. It is not prescriptive in most of its requirements, meaning that organizations must make decisions about which approaches to take. What is the balance between gathering data for analytics and the increased exposure from data minimisation and purpose limitation? What the heck is 'State of the Art' and how do I know if I need it?

Risk awareness starts with self-awareness: what data do I have and how do the new regulations affect how I should treat this data?

STAGE 2: Time to Accelerate

It seems that you are at the developing stages of risk awareness, and are ready to accelerate. You appear to be engaged in asking the right kinds of questions, and they are increasingly sophisticated. You are challenged by some advanced requirements, and seem appropriately concerned about the increased risk levels associated with GDPR. However, your struggle to prioritise resources reflects a need to re-emphasis awareness, particularly at board level.

Your response indicates a mature approach to cloud and data protection. This may involve adapting existing cloud services to make sure they adhere to the new regulations. Or it may be that you have already made sure your cloud usage is compliant, and needs no further changes. If this is true then great: you're ahead of the game. But a word of warning: the consequences of getting cloud usage wrong – for example by assuming cloud providers can absorb liability (they can't) – could be severe. Make sure you have reviewed your cloud contracts and that they are GDPR-ready.

You appear to be quite comfortable with GDPR and have not expressed a high level of concern. Given you are closer to the start of GDPR compliance than the end, have you under-estimated the potential consequences of non-compliance? It will be worth revisiting the risks associated with security breaches under GDPR. It's not all about fines: class action law suits may be initiated by third parties beyond your control of that of the regulator. The regulator itself can order a suspension of data processing, effectively limiting your ability to trade. Overall, GDPR represents a significant increase in the level of business risk related to personal data processing. Make sure your risk assessment function reflects this heightened exposure.

You indicated that conflicting priorities is constraining your ability to create a GDPR program that spans your data management environment. This is typical of organizations in the middle stages of compliance efforts. Ultimately it comes down to an assessment of the risk for your organization. A thorough risk evaluation should identify and resolve conflicting priorities. It may be then that there is a lack of awareness and leadership at board level, resulting in insufficient commitment to GDPR. This is serious, so board engagement is essential if you want to meet your GDPR aspirations.

You indicated that a lack of collaboration between the GDPR compliance team and other stakeholders is constraining your ability to create a GDPR program that spans your data management environment. This is typical of organizations in the later stages of compliance efforts. Your program is well under way, but it may be stuck within one department. A critical success factor for GDPR is cross-functional collaboration: GDPR is too important to stay within fiefdoms.

You indicated that fragmentation of data management systems is constraining your ability to create a GDPR program that spans your data management environment. This is typical of organizations in the later stages of compliance efforts. Your program is well under way, but a fragmented data management environment could be hard to fix: big data and analytics are often critical to business functions. But they can also represent a source of risk, in the volume of personal data held and in the use of that data for multiple purposes. An integrated approach to data governance is essential to efficient GDPR compliance, so focus on this as a core activity in embedding operational excellence in compliance.