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 2: Time to Accelerate

You've got going, but there is quite a way to go still. organizations that fall into this category of defined readiness have made a commitment to GDPR but are still in the first half of their journey. They are aware of the scale of the proposed penalties and sanctions, but are often reluctant to believe that these will be enforced.

By your own admission, you are engaged in enough GDPR activity to avoid a regulator's attention (probably), but are limiting your efforts to a pragmatic program of specific activity. This is a perfectly reasonable strategy, at least in the short term, as long as it is based on a detailed business-lead analysis of research. You are aiming to be pragmatically compliant, so realise that there are risks that remain that you may have to explain to in regulator, should things go awry.

If in doubt, always refer to the principles laid out in Article 5 of GDPR. Be prepared to defend your stance against these principles: if you can do so, then you will avoid the wrath of the regulator.

Your readiness is boosted by the beginnings 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 1: Time to Initiate

Unfortunately, you are in the initial stages of information governance, and you have low confidence in your ability to identify and locate data. You may have a good understanding of structured data, but unstructured information maybe causing difficulty. You are also likely to be gathering data without a real sense of purpose or business value. GDPR now makes this data a risk, so you need to decide whether to keep it or delete it.

According to your score you are likely to struggle to service subject access requests and other new rights introduced by GDPR (including the right to be forgotten).

Your organization remains exposed to a degree of risk because you cannot definitively identify and locate every instance of personal data in your organization. Only you can decide whether this is a risk that your business can accept. Although GDPR demands that you can locate all instances of personal data, you are in the majority of organizations that admit to falling short of this. Assess the risk associated with data that you may not know about, and create an incident response plan for any related potential non-compliance.

In short, you are not data aware. 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 likely be in breach of the principles of purpose limitation, data minimisation and storage limitation. You need to decide whether this is a risk you can live with.

Where to start? Given the pressures of time, you need to prioritise on the data is most valuable to you or that which poses the greatest risk. Any sensitive data (special categories) falls into this area, as does data that would substantially damage your reputation if it was breached. Of course, protecting the data is just one step, so you also need to focus on the processes that interact with the data. Defining who has access to what data, and for what purpose, is mandatory.

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.

IDC's GDPR Readiness Assessment & Recommendations

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 1: Time to Initiate

It seems that you are at the initial stages of risk awareness. You appear to be engaged in asking the right kinds of questions, but they are foundational. You are challenged by some basic requirements, and seem less concerned abut GDPR than would otherwise be expected with a full knowledge of the regulations. Your struggle to gather budget and resources reflects a low level of awareness, particularly at board level.

Your response shows that you are actively trying to square your cloud usage with GDPR requirements. Good: GDPR places new obligations on data processors, which includes all cloud services. You seem especially concerned at the international data transfer rules. In fact, there is little change to the existing rules that allow data transfers, as long as there is adequate protection in place. Remember that it is perfectly possible to be compliant with GDPR while using cloud services. Cloud service providers are aware of their obligations, and many are offering GDPR-ready contracts.

You appear to have balanced perspective on the risks associated with GDPR. This means that you fully understand the potential impact of non-compliance, not just in terms of possible fines but reputation damage, class action law suits and suspension of data processing. But you are still in the early stages of GDPR compliance – keep moving forwards.

You indicated that a lack of budget is constraining your ability to create a GDPR program that spans your data management environment. Budget issues are unfortunately not very easy to fix. Ultimately it comes down to an assessment of the risk for your organization. But a lack of awareness will inhibit a thorough risk evaluation. Information leads to enlightenment, and enlightenment should lead to a break in inertia. There's nothing like an increase in perceived risk to loosen fiscal ties.

You indicated that limited resourcing 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 the need to dedicate and fund the required resources. 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.

IDC's GDPR Readiness Assessment & Recommendations

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.