IDC's GDPR Assessment: Endpoint Readiness
Introduction

GDPR is Coming

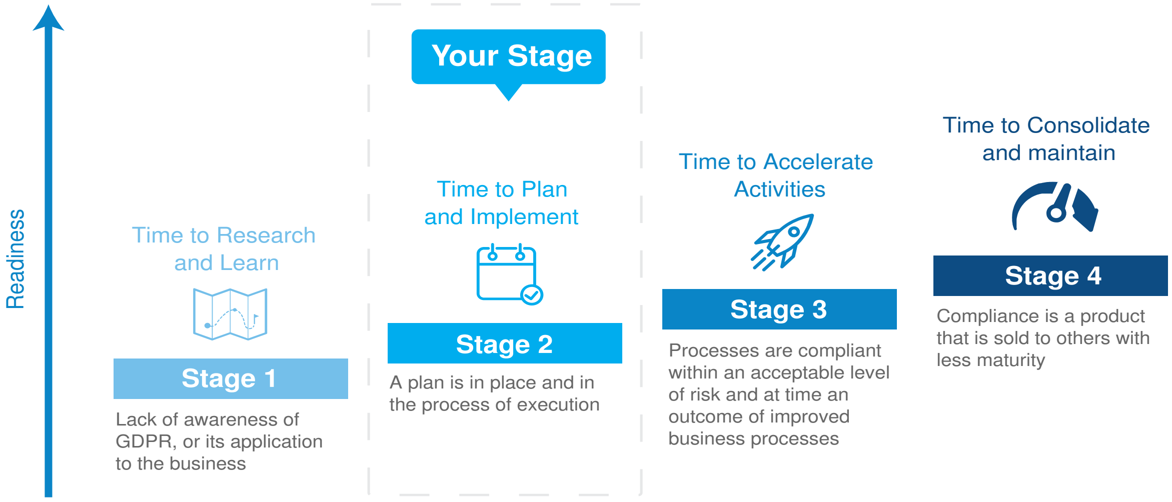
Are your devices ready for GDPR compliance?

Introduction

Thank you for taking part in IDC's GDPR readiness assessment for endpoint devices. This study enables you to assess your organisation's readiness, based on IDC's in-depth understanding of the GDPR requirements and the roadmap to compliance. It also provides you with essential guidance in the development of your security strategy. This includes recommendations on how to progress your organisation towards a compliant and sustainable position in preparation for May 2018.

Based on IDC's assessment, your organisation is at **Stage 2: Time to Plan and Implement** in terms of its overall readiness to address GDPR in general, in your hardware estate and specifically with regards to your print infrastructure and printer fleet.

Further insight and detailed recommendations are highlighted below, taking you through components of Leadership and General Obligations, Data Rights and Standards, as well as Security. The report delivers an assessment of your stage of readiness as well as individual recommendations on how to improve these areas.



Readiness

Your Stage

Time to Research and Learn

Stage 1

Lack of awareness of GDPR, or its application to the business

Time to Plan and Implement

Stage 2

A plan is in place and in the process of execution

Time to Accelerate Activities

Stage 3

Processes are compliant within an acceptable level of risk and at time an outcome of improved business processes

Time to Consolidate and maintain

Stage 4

Compliance is a product that is sold to others with less maturity

GDPR and Print

The EU General Data Protection Regulation (GDPR) is now in force with a transition period until May 25, 2018. IDC research shows that many organisations 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.

GDPR compliance is required by any organisation — 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. Outputting of personal data including printing, copying, faxing and scanning is considered as processing and is subject to GDPR regulation.

For example, if paper is used as part of a system to store or output personal data, this is also covered by the GDPR regulation. For many organisations, this is new or at the very least confusing. For others, progress has already been made and some will look to utilise the process of compliance in driving other benefits such as cost-cutting, improved security and environmental concessions to the wider organisation. While you still have time, the clock is ticking and the requirements are wide reaching. Good luck.

Overall Readiness

STAGE 2: Time to Plan and Implement

Organisations that fall into this category of defined readiness often have patchy or scant knowledge of GDPR in general, or how this impacts their endpoint devices and print estates specifically. They are somewhat aware of the scale of the proposed penalties but are reluctant to believe that these will be enforced.

They may also be rushing around in blind panic, with no sense of prioritisation or focus. They are aware of general IT and print security standards, but have not made a concerted effort to define a print security process or seek security certification. Understanding of their organisation's data processing activities may also be very limited.

Those with a greater understanding of the requirements need to step up the frequency of some of their testing efforts. IDC has outlined some key recommendations to address these points below.

Recommendations for Planning Businesses

Okay, good. You're aware of GDPR and its implications. That makes you ahead of many companies already. But there's a long way to go. You're in a state of dawning realisation and with the deadline for compliance looming you need to prioritise. A review of your endpoint devices should be on your agenda, and print is a good place to start — you can make substantial gains quickly, and avoid possible catastrophic data leakages from printed material now and in the future.

You may have started documenting data flows across your IT infrastructure — good. But for many organisations in this stage of readiness, print may be a blind spot, so you need to be sure to add it into your data maps. You also need to assess why you're allowing people to print personal data. There are plenty of legitimate reasons why people print personal data — forms, CVs, emails and so on — but typically this would be for specific purposes, by authorised individuals. Printing the customer database is unlikely to be such a case (more likely an insider threat), nor is printing employee salaries (most likely poor HR practice). GDPR requires that you document why you process personal data, so you need to document why you print it.

Generally, you should ensure that your printer fleet matches the security specifications of other endpoint devices, such as PCs and tablets. What are the security characteristics of your printer fleet? Is it ISO/IEC 15408 certified? This standard, often referred to as the Common Criteria, is a benchmark in security of a variety of devices, but although certified printers are available few are deployed. Are the communications ports in your printers secured? Most are left wide open, leaving printers vulnerable to elementary probes and attacks. Do your printers offer additional authentication (e.g., a PIN) before printing a document from the spooler?

Reviewing your print processes may seem dull, or trivial, compared with the mounting priorities from other data sources. But printed information remains a key vector for data breaches, and it also acts as an indicator of good practice to auditors and regulators. With some immediate attention, you can shift your readiness substantially up the chart.

Further insight based on the dynamics of Leadership and General Obligations, Data Rights and Standards, as well as Security, are outlined in more detail below.

Leadership and General Obligations

STAGE 1: Time to Research and Learn

Organisations at this stage in the process of GDPR often do not have a process that mandates the consideration of data protection when conceiving and deploying new technology, design or business processes. Often, they do not restrict personal data access to those that are required to have access to that data. Perhaps your board is unaware of its accountability for GDPR compliance, or is yet to do anything to address the forthcoming requirements? Even if it is aware of the enforcement, perhaps it doesn't know about the fines or sanctions?

Critically, you may not understand how hardware such as PCs, laptops, smartphones, servers and removable storage objects as well as printers, copiers, faxes and general document management process relate to GDPR regulation. Organisations at this stage in their GDPR journey do not even have a grasp of the reach and ramifications of GDPR and endpoint devices.

Without at least a rudimentary understanding of the regulation and how to prepare for compliance the task seems almost insurmountable within the timeframe unless you act now. Immediate objectives and measures are needed to create awareness, develop understanding and begin the planning process.

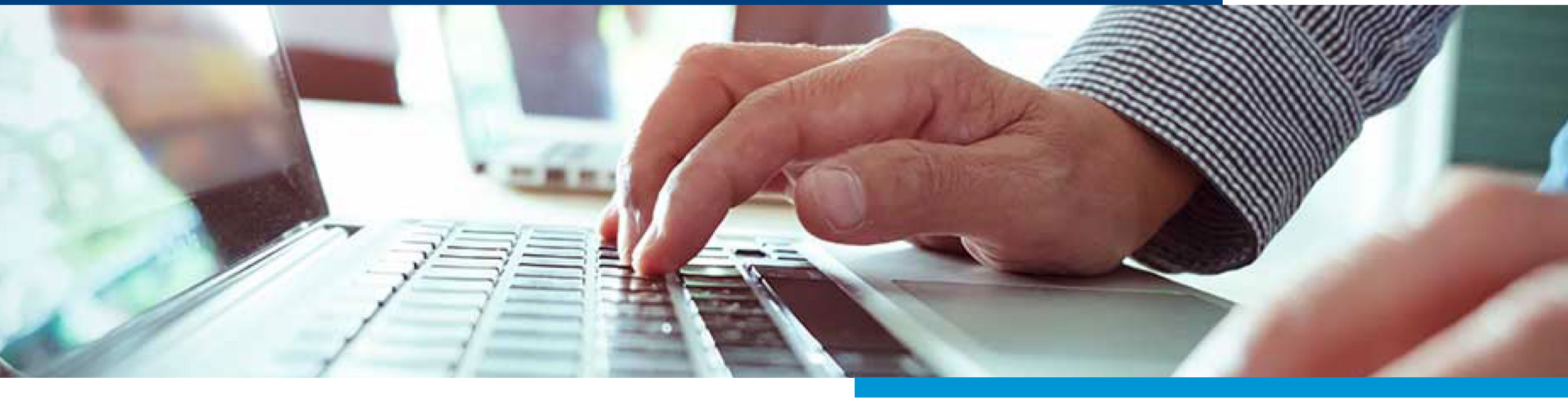
Recommendations and Actions

Your organisation and the board need to establish a full understanding of the implications and requirements of GDPR compliance. Part of this process is understanding the consequences of failing to comply, as well as a clear roadmap and timelines involved.

Specific to the print and elements of the business, you and the board must define and follow a comprehensive GDPR plan, considering all aspects of print management and the control and process of personal data throughout the organisation.

One way to address this quickly is to assess and audit your IT infrastructure and hardware estate, along with your general approach to document management, storage and authentication. These are key entry points for external security threats, and are also vulnerable to insiders, whether operating accidentally or through malicious intent. Print is particularly susceptible to insider action, as it is rarely monitored closely. The first step in securely managing and monitoring the printer hardware fleet is to establish a baseline by building an understanding of what devices you have, what you need and what you need to do to comply. A refresh of policy and the way your organisation manages and utilises print will address many immediate and fundamental requirements, allowing you to plan for the next 12 months.

While GDPR is a very large stick with which to enforce (often much needed) change, the wider benefits of a technology refresh must also be presented and supported. Moving your way up through the readiness maturity levels is one way of managing this approach and understanding your progress. Thus, IDC invites you (and the board members) to retake this test in a few months' time, measuring and maintaining a focus on achieving compliance and realising the benefits of such an approach.



Data rights and standards

STAGE 2: Time to Plan and Implement

Your organisation is kind of a half-way house on the way to compliance. While your organisation understands what kind of data is collected, why data is collected and where it is stored, there is no real consideration of local storage regulation links that apply to specific geographical locations. There is also no strict purpose and process linkage in place. Some ad hoc and fragmented data flow analysis has taken place and there is a process in place to ensure the secure movement and outputting of data. While you may claim to be adherent to the basic principles and spirit of ISO 27001 and ISO/IEC 15408 this is not enough to be officially certified.

Organisations at this stage in their GDPR journey do not yet have a formalised plan. Some may be reacting on a piecemeal basis; others will be hoping for loose interpretations of the regulation.

Having a half-hearted approach will not spare you non-compliance fines. In fact, it is likely to exacerbate sanctions. Objectives and measures are required to stiffen your resolve and leverage what you have already to push on and achieve full compliance.

Recommendations and Actions

Your organisation could go either way: you could press on from what you have done already and comply fully with the regulation or you could bank on being good enough and hope for a lenient audit. Seek out some examples of high-profile data breaches and the subsequent hard and soft costs to the organisations concerned and present them to your board. This may be what is required to persuade them to divert resources to a GDPR compliance project.

Specific to print, revert to your supplier and invest in (ISO/IEC 15408) certified devices. Newer devices with this certification will not only be more secure but they will have other environmental, cost-saving and process improving features and benefits associated with newer technology. But think beyond just replacing hardware to implementing a secure print solution instead.

Security

STAGE 2: Time to Plan and Implement

From IDC's assessment, it appears as if you're on your way to compliance; your print devices are as secure as they can be now, but print needs to be embedded deeper into your overall processes. With regards to backup and testing processes, these fall short of what is required to pass muster.

Organisations at this stage in their GDPR journey need to implement more regular and stringent processes (including print) every step of the way.

Your organisation is already very security minded. Objectives and measures are required to take that thinking to the next level to meet the regulation requirements.

Recommendations and Actions

Your organisation is doing most of the right things; it just needs to do them more often and in a more formal way. Introduce more frequent backup testing and formalise regular incident response plan testing.

Print is a crucial part of the GDPR process and to that end you must insist that print is part of the security audit and that encryption processes apply to print. You must also ensure that you log all printing activities to enable tracing. Finally set up a process to define and review state-of-the-art security.

It's also worth at this stage reviewing your print-related activities against the broad principles of data protection. Unauthorised access of personal data is a primary example: you need to demonstrate control over this area, including maintaining an audit trail of access attempts. Did someone try to access a document in the printer queue? How can you tell if they did? Could you prove that no one did, or could?