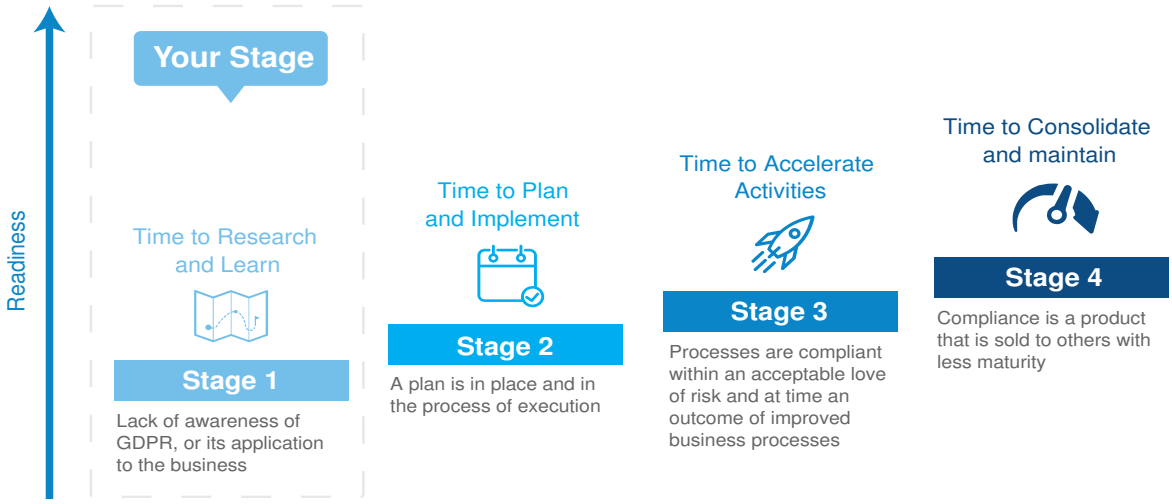
IDC's GDPR Readiness Assessment Report
Introduction

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 1: Initial** 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.



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 GDPR and Print Maturity

STAGE 1: Time to Research and Learn

Organisations that fall into this category of initial readiness often have limited or no insight into the requirements and (more importantly) the implications of GDPR on their business. Leadership does not have any real understanding of what GDPR covers and how it is to be implemented. In addition, there is often no real understanding of legal obligations and accountability, or the extent of the fines and other sanctions if the business fails to comply by May next year.

In short, you are largely unaware. Even with a basic understanding of the scope and content of GDPR, many in this category have little understanding of its requirements and (in particular) how it relates to devices such as PCs and printers. You may well have little or no access or authentication mechanisms at the device itself, leaving data open to loss or simply unprotected in the work environment.

This weak link could become the organisation's undoing — with print and MFP devices often a forgotten part of the estate, you may not have basic Common Criteria (CC) certification. Importantly, it is not just a data breach that results in non-compliance. A lack of adherence to the basic principles and rights of data protection are equally critical to achieving compliance.

In terms of data collection, your organisation is probably yet to formally identify personal data types held within the organisation. More specifically, the elements of data types classed as personal data and those that are not may well be unclear, and you are unlikely to be aware of the extended obligations relating to special categories of data (i.e., sensitive data). This is basic stuff: a core requirement of GDPR is that you know what personal data you have, where it is and what sensitivity it involves.

You are also unlikely to have defined a security incident response plan or agreed policies for transferring data. Perhaps you didn't know you needed to do this, or perhaps you were unaware of the extent of the requirement. In short, don't panic. By filling this survey in, you are already in a better position and you have time to act. In response, IDC has outlined some key recommendations and a roadmap for addressing GDPR and print.

Recommendations for Learning Businesses

Quickly, but calmly, bring GDPR to the attention of your board. Use this report to set out the various areas for attention and emphasise the need for action now: not only at a general level, but also specifically for endpoint devices and print.

Be sure to communicate that GDPR will be enforced worldwide. Brexit will not save the business from needing to do this as the regulation applies to the personal data of EU data subjects regardless of the location of the controlling and processing entities. Make sure your organisation is aware that random spot checks are likely and this approach is already happening.

Perhaps the board is aware of GDPR and is implementing changes, but again board members may not be aware of the wider implications around print. Make this point clear. Any weakness in the approach will lead to a failure of compliance. Even if this does not result in a breach, fines and sanctions will still apply. Very few printers are secured and the most obvious elements of storage, networking and computing will divert attention.

Your organisation still needs to define "state-of-the-art" security. You are not obliged to implement state-of-the-art, but you do need to document your understanding of it, to then justify why you did, or did not, deploy it. Ensure that you are working towards this, while plotting and mapping the risks related to print and the management of personal data.

Other key action points include consideration of defined and secured print process. This should cover the rationale for the

ability to print personal data: have you documented the cases in which you allow this to happen? Sensitive data should rarely, if ever, be printed. Can you control this?

Can you determine that only the person authorised to print personal data can then collect it from the printer? What security mechanisms exist on the printer itself? Can you detect someone in a non-EU country printing personal data (which would constitute a data transfer)? Is the physical storage in the printer encrypted?

By thinking through the information flows in your organisation and relating these to print, you should be able to identify the main compliance vulnerabilities and plan remediation. 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.

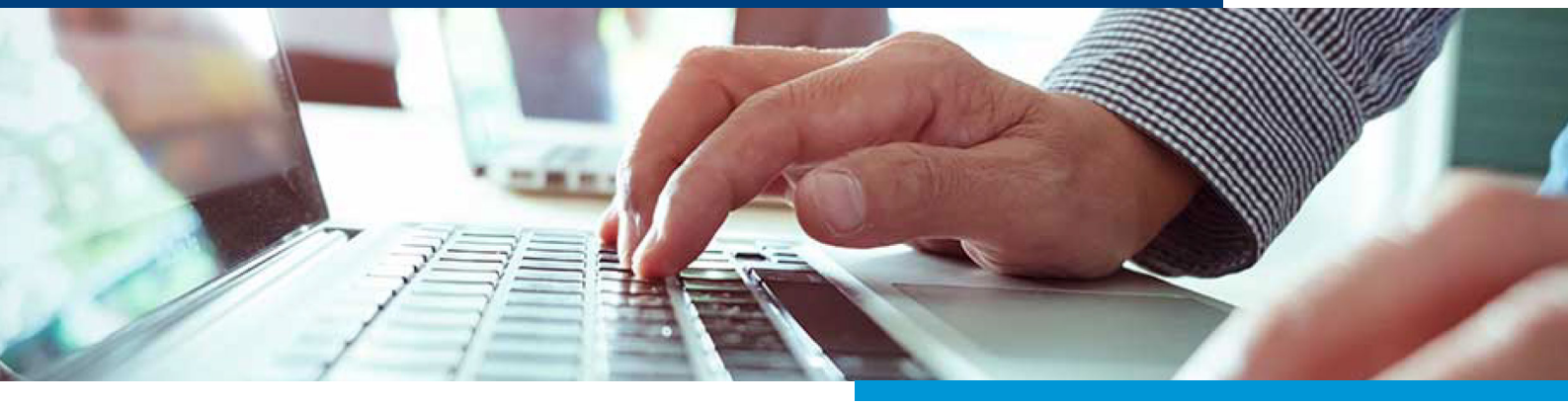
Recommendations and Actions

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 1: Time to Research and Learn

For organisations at this stage in their security readiness, the GDPR regulators would most likely consider you unsecure, given the current state of your processes. In addition, you probably have little or no measures in place to safeguard personal data as it travels through your endpoint and print devices. You have likely not taken even the simplest steps to ensure that your print infrastructure and printers are shooting for state of the art with regards to security.

Organisations at this stage are at the very beginning of not only their GDPR journey but also their overall security journey. Remedial action must be taken now for you to have any chance of becoming compliant by the deadline and avoiding those hefty penalties.

Immediate objectives and measures are needed to understand what you can do to shore up your print devices thus making them secure and fit for purpose in general but also to specifically qualify as aiming for state of the art in terms of GDPR security. State of the art is not mandated, but it's best practice to know what it is and to document why — or why not — modern technologies were deployed.

Recommendations and Actions

The bad news is that you are very far from understanding and aiming for state of the art, but the good news is that in terms of your print devices there are several tactical changes that you can easily make to help you improve your security status. Firstly, you can ensure that you compile and manage a complete inventory of your print devices, that you maintain and patch your printer fleet, that you shut down any unnecessary services that your print devices offer and that you properly erase or destroy any hard disk drives (this applies to all hardware types, not just printers).

On a strategic level, you can include print infrastructure in your security audit and in your personal data encryption process. First, though, you must have an encryption process if you don't have one already.

One of the key components of the security section of the regulation is documenting the risks associated with processing personal data, and mapping those risks against the technical measures in place to secure personal data. Failing to do this means failing to comply. Other critical components revolve around testing: testing security, backup, business continuity and key management processes and having and testing an incident response plan. Being able to evidence these processes will help your case as being state of the art in security. One of your first steps must be to formulate and implement that incident response plan.