aiim Industry Watch

Delivering the priorities and opinions of AIIM's 155,000 community

aiim

GDPR after the Deadline —

Progress, But a Long Way to Go

In Partnership with

DOCAUTHORITY

ABOUT THE RESEARCH

As the non-profit association dedicated to nurturing, growing and supporting the information management community, AIIM is proud to provide this research at no charge to our members. In this way, the entire community can leverage the education, thought leadership and direction provided by our work. We would like these research findings to be as widely distributed as possible.

Feel free to use individual elements of this research in presentations and publications with the attribution — "© AIIM 2018, www.aiim.org". Permission is *not* given for other aggregators to host this report on their own website.

Rather than redistribute a copy of this report to your colleagues or clients, we would prefer that you direct them to www.aiim.org/research for a download of their own.

Our ability to deliver such high-quality research is partially made possible by underwriters, without whom we would have to use a paid subscription model. For that, we hope you will join us in thanking our underwriters:

aiim Industry Watch

Delivering the priorities and opinions of AIIM's 155,000 community

TABLE OF CONTENTS

PROCESS USED AND SURVEY DEMOGRAPHICS

About AIIM

Here at AIIM, we believe that information is your most important asset and we want to teach you the skills to manage it. We've felt this way since 1943, back when this community was founded.

Sure, the technology has come a long way since then and the variety of information we're managing has changed a lot, but one tenet has remained constant — we've always focused on the intersection of people, processes, and information. We help organizations put information to work.

AIIM is a non-profit organization that provides independent research, training, and certification for information professionals. Visit us at www.aiim.org.

About the author

John Mancini
Chief Evangelist and Past President of AIIM

John Mancini is the Chief Evangelist and Past President of AIIM. He is a well-known author and speaker on information management and digital transformation.

As a frequent keynote speaker, John offers his expertise on Digital Transformation and the struggle to overcome Information Chaos. He blogs under the title Digital Landfill (http://info.aiim.org/digital-landfill), has more than 11,000 Twitter followers, 6,000 Linkedin followers, and can be found on most social media as @jmancini77. He has published more than 25 e-books, the most recent being:

- 2017: A Digitally "Transformative" Year
- The State of Intelligent Information Management: Getting Ahead of the Digital Transformation Curve
- Information Privacy and Security: GDPR is Just the Tip of the Iceberg
- From ECM to Intelligent Information Management
- 10 Strategies to Navigate the Shift from ECM to Content Services

ABOUT THIS SURVEY

We greatly value our objectivity and independence as a non-profit industry association. The results of the survey and the market commentary made in this report are independent of any bias from the vendor community.

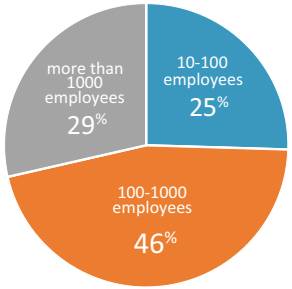
The survey was taken using a web-based tool. Invitations to take the survey were sent via email to a broad base of names associated with AIIM. They are therefore interested in some way with information and content management, but not necessarily AIIM members. The link was also posted in a variety of social media outlets.

A total of 262 individuals participated in the survey. Core demographics are reflected in the charts that follow. Portions of the commentary are quoted from the AIIM eBook Information Privacy and Security: The GDPR is Just the Tip of the Iceberg by John Mancini and Andrew Pery.

Significant representation — 46% — from mid-sized market.

Note: There is a higher % of large companies in the US sample (see sidebar).

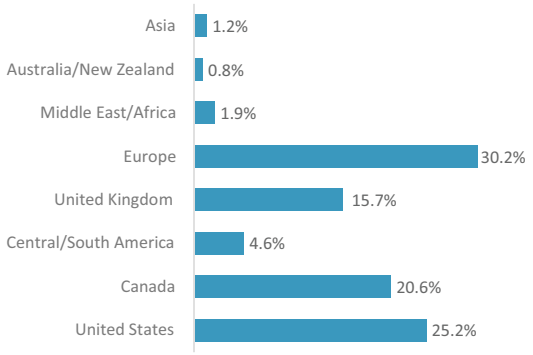
Number of employees



	10-100 employees	100-1000 employees	more than 1,000 employees
US	10.9%	42.2%	46.9%
UK	41.5%	41.5%	17.1%
Europe	39.7%	39.7%	20.5%

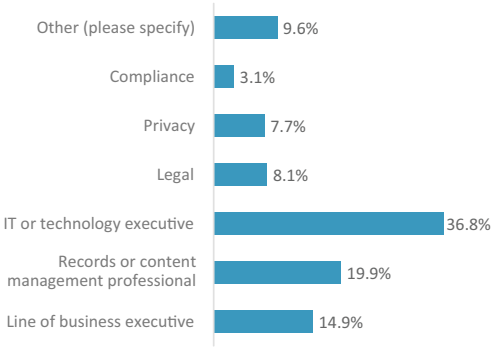
46% from Europe and the UK; 46% from North America.

Location



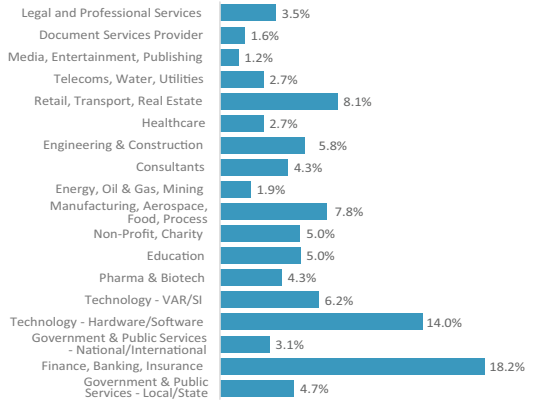
37% from IT, 20% from RM/ CM, 19% from privacy, legal and compliance.

What kind of work do you do?



Largest segments = financial services, technology, government, retail, manufacturing

What industry are you in?



PROJECT OBJECTIVES

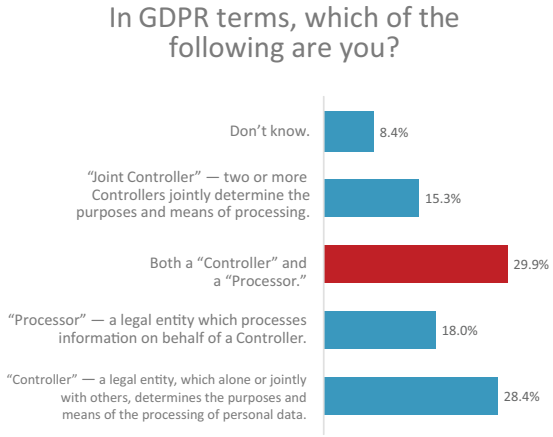
Project Background

Today, consumers are subject to unprecedented incursions to their privacy. The juxtaposition of big data, cloud computing, predictive analytics and the Internet of Things enables organizations to collect and process vast amounts of information about them. Taken together, these create a digital fingerprint of behaviors that may expose personally identifiable information. There seems to be a sense of capitulation among consumers and business that in this digital age, privacy rights are destined to erode — and in response, governments and regulators are stepping in.

Historically the EU has had a high bar for privacy protection. Privacy is considered to be a fundamental human right and Article 7 of the EU Charter of Human Rights stipulates that "everyone has the right to respect...private and family life, home and communications." EU Privacy initiatives — including the EU Privacy Directive that preceded the European General Data Protection Regulation — are based on the preservation of privacy rights as an immutable principle.

The General Data Protection Regulation (GDPR) was a response to: 1) advances in digital technologies such as big data, cloud computing, and predictive analytics; and 2) revelations of bulk data collection and profiling by intelligence services. The result is a comprehensive overhaul of privacy legislation and a considerable strengthening and expansion of privacy rights.

30% of organizations act as BOTH a "controller" and a "processor."



The GDPR's May 25, 2018 deadline set in motion a mad compliance and security scramble not only for European companies, but also for any company doing business in Europe or with European customers.

The purpose of this survey was to quantify — as close to the May 25th deadline as possible – the following three key issues related to GDPR:

- How do organizations view the emerging challenges tied to information privacy and security, and whom have they charged with this task?
- At the deadline, where are organizations in their GDPR journey and how much did they spend to get there? How do they assess their progress in meeting the core requirements of GDPR?
- What kinds of special pain points does unstructured information (i.e., content) raise in GDPR compliance efforts, and which core IIM technologies do organizations see as critical to their efforts?

1. How do organizations view the emerging challenges tied to information privacy and security, and whom have they charged with this task?

The scope of GDPR includes more rigorous consent requirements, data anonymization, the right to be forgotten and breach notification requirements. Violations could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year – whichever is the greater — being levied by data watchdogs. For other breaches, the authorities could impose fines on companies of up to €10m or 2% of global annual turnover — whichever is greater. For the average Fortune 500 company, that puts fines in the range of $800-900M.

But the impact of GDPR really goes beyond the immediate need to be compliant. The GDPR reflects an emerging consensus that the rules and practices and technologies used to manage the security and privacy of personal information need to evolve to reflect the explosive growth of this information and the increasing sophistication of the tools to manage it.

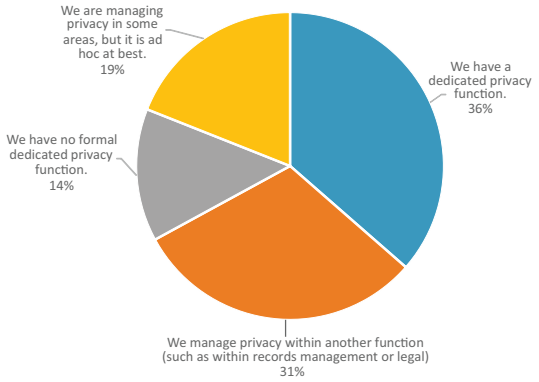
Key Findings

- Information privacy is still an afterthought for most organizations. Only 36% of organizations have a **dedicated** privacy function — a key factor in determining accountability. The other 64% either lodge responsibility in another function or have no privacy function to speak of.
- For nearly 40% of organizations, the primary reason to focus on GDPR is because **they have to** — it's a legal obligation. Missing from this fairly practical calculus is the fact that a strategic and focused approach to information management and information governance is not just good hygiene – it sets the stage for machine learning and artificial intelligence.
- There are a **variety of accountability models for GDPR**, with no clear winner: IT is responsible in 27% of organizations, followed by LOB (finance and operations, 19%), RM/Information Governance (15%), Legal (15%), and Compliance (13%). For AIIM audiences, the relatively low percentage of organizations that place GDPR responsibility with RM/IG perhaps reflects a long-term shift for this function in the direction of IT.
- Fear of **additional regulatory scrutiny** — somewhat akin to the fear that an IRS audit frequently leads to additional audits — is the primary worry for 32% of organizations should they suffer a compliance lapse.

GDPR AFTER THE DEADLINE

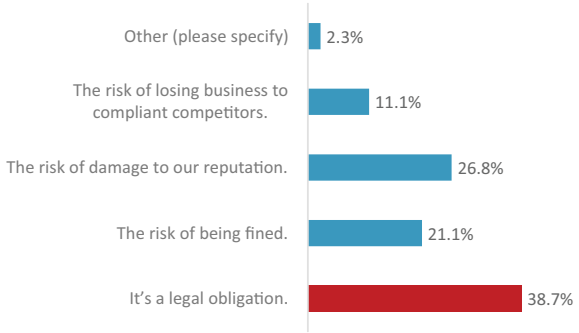
Why? — Privacy lacks a dedicated focus for 64% of organizations.

How is privacy handled in your organization?



Why GDPR? – We have to.

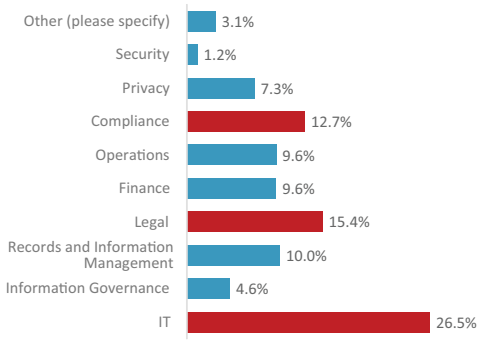
What is the primary reason for your organization's investment in GDPR compliance?



Who is on the hook for GDPR?

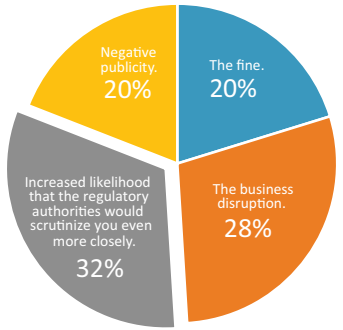
A variety of models for who is responsible and no clear best practice.

Which of the following departments has PRIMARY responsibility for leading your GDPR compliance effort?



"Fear of regulator scrutiny" and potential business disruption the biggest concerns.

If you were to suffer a GDPR compliance issue and were brought before the regulatory authorities, what would be the MOST damaging aspect in your opinion?



2. At the deadline, where are organizations in their GDPR journey and how much did they spend to get there? How do they assess their progress in meeting the core requirements of GDPR?

Prior to the May 25 deadline, there was a wide variety of reporting about how prepared organizations would be:

- "Overall, only 15% of organizations surveyed expect to be fully compliant by May 2018, with the majority instead targeting a risk-based, defensible position." (Deloitte, 2017)
- Only 43% said they were "very confident" about the core processes their company had in place to comply with GDPR requirements (Forrester, December 2017).
- "A joint survey issued by law firm McDermott Will & Emery and the Ponemon Institute found that just over half of respondents, 52%, said their organizations would be ready by the deadline."
- "While 11% of organizations are completely prepared for GDPR (i.e., would be ready if it went into effect tomorrow), 33% say they are mostly prepared (i.e., most work done but some tasks left to accomplish), and 44% claim they are somewhat prepared (i.e., organization has identified all the steps to meet the GDPR deadline but are early in the process of completing all tasks)." (CSO Online)

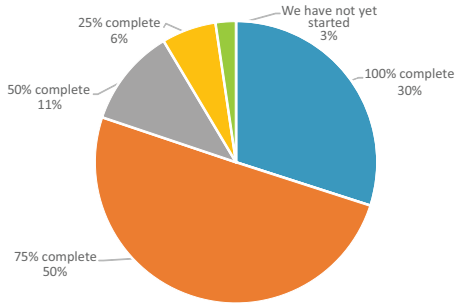
Key Findings

Our findings suggest somewhat of a "good news/bad news" story with regards to the progress organizations had actually made by the deadline:

- Only **30% of organizations said they were 100% ready** by the deadline, a bit lower result than was forecast by many prior to the deadline. A further discouraging note is that one in five organizations (21%) had yet to identify a Data Processing Officer.
  - On the positive side, an additional **50% said they were 75% of the way toward their objective.** This likely reflects a realization by many that they needed to prioritize areas where exposure was greatest. The most common initial steps taken by organizations were 1) examine and recast all of their contractual terms; and 2) get outside assistance in doing so.
- The level of budget dedicated to GDPR compliance is significant, reinforcing many predictions that this was indeed a watershed event. **33% of organizations said their GDPR compliance budget was in excess of €1 million; 15% said it was more than €10 million.**
- The average GDPR budget was €3.5 million; the median was €500,000.
- Companies in the US and the UK reported a significantly higher GDPR budget than their European counterparts, perhaps reflecting a stronger initial privacy starting place for European companies.

Only 30% of organizations compliant at the May 25th deadline; but another 50% almost there.

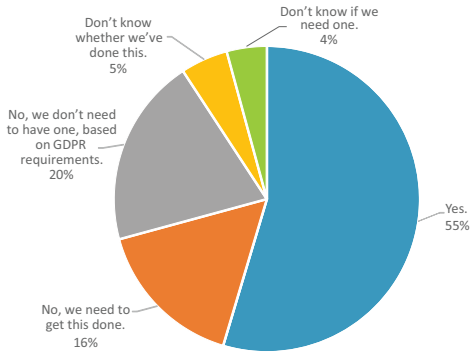
Having completed this survey, please think about ALL of the various GDPR compliance requirements that went into effect May 25. Where are you on the journey to be 100% compliant?



GDPR AFTER THE DEADLINE

26% of organizations still need to appoint a DPO – or have no idea of whether they need to or not.

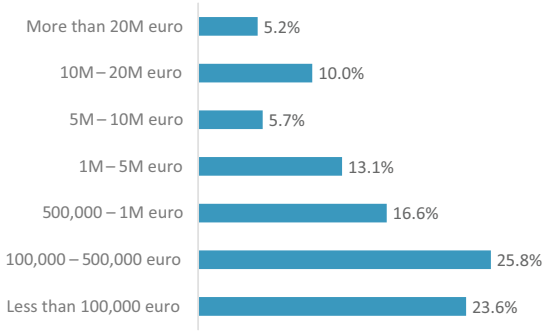
Have you appointed a "Data Processing Officer"?



Average GDPR budget = 3.5M euro

Median GDPR budget = 500K euro

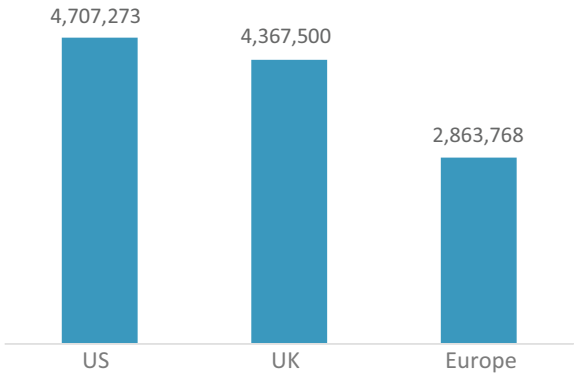
What kind of budget does your organization have for GDPR compliance?



Higher average GDPR budgets outside Europe –

Does this reflect a stronger privacy starting point for European companies?

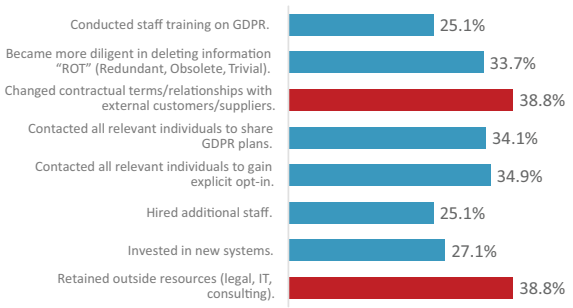
Average GDPR budget



Step 1 – change contract terms.

Step 2 – Get outside help.

Which of the following did you do as part of the run-up to the May 25 GDPR deadline (check all that apply)



3. What kinds of special pain points does unstructured information (i.e., content) raise in GDPR compliance efforts, and which core IIM technologies do organizations see as critical to their efforts?

For organizations at significant scale — most of those in our survey — GDPR poses challenges that seem not that difficult on the surface, but are actually quite complex.

As an example, consider the right of customers to be provided a machine-readable version of ALL of the information handled by a company. For relatively small companies, this is likely a process that *could* be handled manually if necessary; the volume of requests is likely to be small, as is the number of systems in which personal information is likely to be contained.

But at scale, consider the number of places that data and content about a fictional "Mary Smith" is likely to be found. Consider how disconnected most of these systems are — the challenges most organizations have with relatively simple case management provide a good example of the complications created by disparate and disconnected systems.

Now consider how many unique ways "Mary Smith" is likely to be identified in these systems. Sometimes "Mary Smith." Sometimes by her maiden name, "Mary Jones." Sometimes by her email address; in all likelihood *multiple* email addresses. Sometimes by her account number. Sometimes by a variation of her name like "M. Elizabeth Smith." The potential complications associated with what seems a relatively simple task on the surface are mind-boggling.

Now consider how many of these kinds of requests an organization at significant scale is likely to get in the course of a year. There is some speculation that individuals with a grievance against a particular company might use social media to "flood" a company with requests — somewhat akin to a denial of service attack.

Lastly, as those in the content space know, there are well known challenges associated with finding and managing personal information within the vast troves of **unstructured** information that are much more complex than those on the **structured** data side of the house.

Key Findings

- **20-30% of organizations have little or only marginal confidence in their ability to meet core GDPR compliance requirements.** Particularly problematic are requirements dealing with 1) proving compliance in an audit context; 2) generating clean and auditable records of processing activities; 3) meeting the 72-hour regulator breach notification requirement; and 4) cross border transfers.
- **20-30% of organizations also have little or only marginal confidence in their ability to respond to the new customer rights created by the GDPR.** Particularly problematic are: 1) the right to be forgotten; 2) the right to data portability and be provided a machine-reading file of all personal information; and 3) the right to object to the processing of data.
- **Over 30% of organization have little or only marginal confidence that the personal information in their core content systems is under control.** Shared drives, SharePoint repositories, and content lodged in third-party SaaS application are particularly challenging.
- With regards to the right to be forgotten, only 40% of organizations have automated processes in place to delete personal information within these systems.
- 39% of organizations have no idea how much it will cost to find all of the information they have about a particular individual (to meet the right to data portability). For those who DO know, 48% believe this seemingly simple right will cost more than €5,000 **per request.**
- On average, companies expect 60.1 GDPR data requests in first 12 months, with average cost of €4,604 EACH. This means an average operating cost of over €276,700 simply to meet the core GDPR rights tied to identifying and accessing personal information.
- 60% of organizations believe the GDPR core requirements relative to website content and processes are under control — which means 40% either believe they are not or have no idea. *[Author's note: Even the 60% is likely to prove an overly optimistic number once organizations experience the complexities that are involved.]*

GDPR AFTER THE DEADLINE

The weakest links…

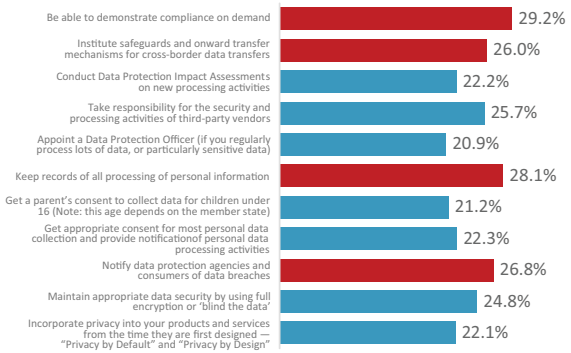
1 – proving compliance

2 – clean records of processing

3 – breach notification

4 – cross border transfers

How confident are you that you have employed the following as part of your GDPR-compliance efforts? (% "not confident" or only "somewhat confident")



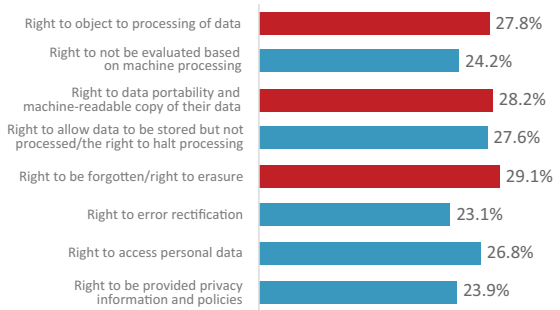
The weakest links…

1 – providing machine-readable data

2 – responding to processing objections

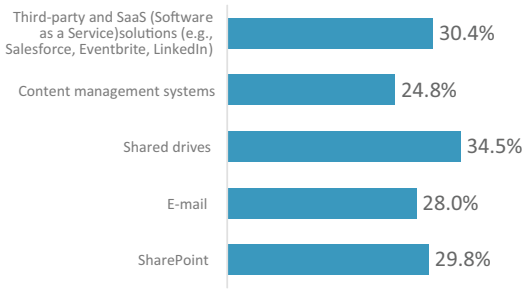
3 – right to be forgotten

How confident are you that your organization has policies and processes in place to protect the following GDPR Data Subject rights? (% "not confident" or only "somewhat confident")



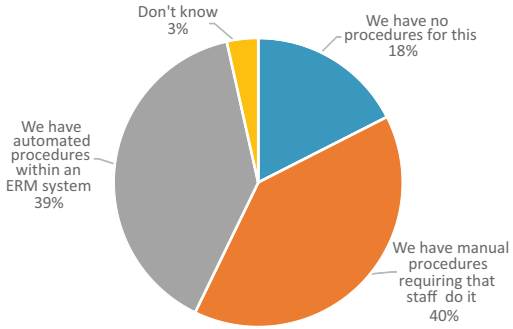
Shared drive, SaaS and SharePoint content particularly problematic under GDPR.

How confident are you that the personal data in the following systems is under control and in compliance with the GDPR? — % "not confident" or "somewhat confident"



Only 40% have automated processes to insure deletion of personal information.

How do you ensure that personal information in email, SharePoint, shared drives, etc. is deleted when appropriate?



GDPR AFTER THE DEADLINE

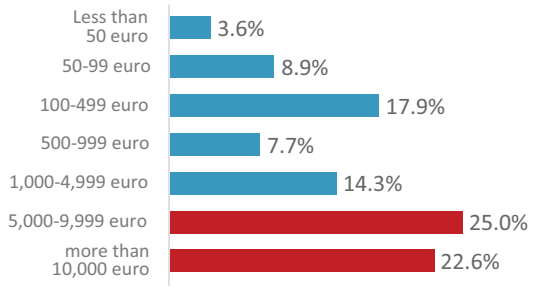
10% – "It's not possible to calibrate costs."

29% – "We have no idea how much this will cost."

47.6% – More than 5,000 euro per instance.

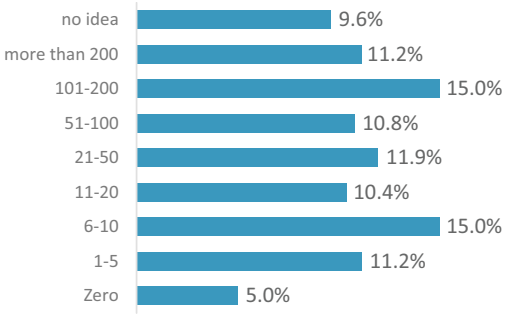
Average = 4,604 euro EACH.

EACH TIME IT OCCURS, about how much will it cost (including cost of staff of staff and 3rd parties) to find ALL of personal information about a former or current employee or customer — Data shows only those who KNOW



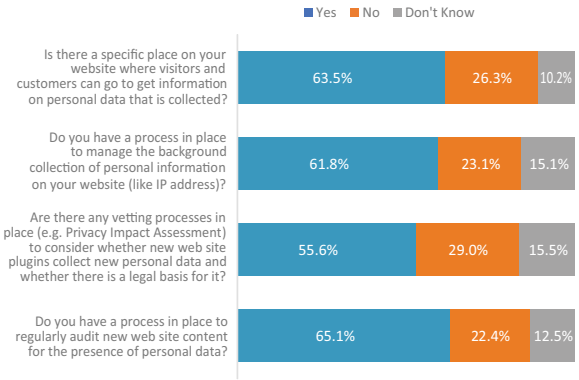
On average, companies expect 60.1 GDPR data requests in first 12 months, with average cost of 4,604 euro EACH – an estimated net annual operating cost of 276,700 euro.

How many subject access, data portability and/or erasure requests do you believe you will receive in the first 12 months of GDPR?



Gut feeling – organizations are more optimistic about their web site compliance than they should be.

GDPR and web site management



Key IIM technologies for GDPR…

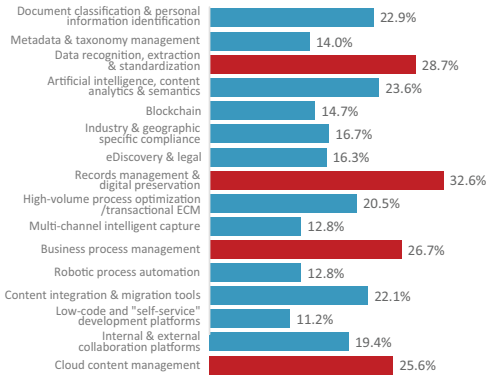
1 – ERM

2 – Automated recognition & extraction

3 – BPM

4 – Cloud content management

Which of the following Intelligent Information Management technology capabilities do you see as MOST critical to your GDPR compliance program? (Please click the 3 MOST IMPORTANT.)



Some Final Thoughts

We are gathering information at unprecedented scale — this isn't new. What is new is that for the first time we have tools to actually make sense of it.

For the most part, we haven't thought through the ethics of what all of this unprecedented accumulation of information — plus the unprecedented new tools to analyze it — actually means. Until we do, we will continue to careen from one privacy crisis to another, and from one ham-handed political response to another. GDPR is not just a temporary annoyance. It reflects a fundamental tension that has yet to be resolved.

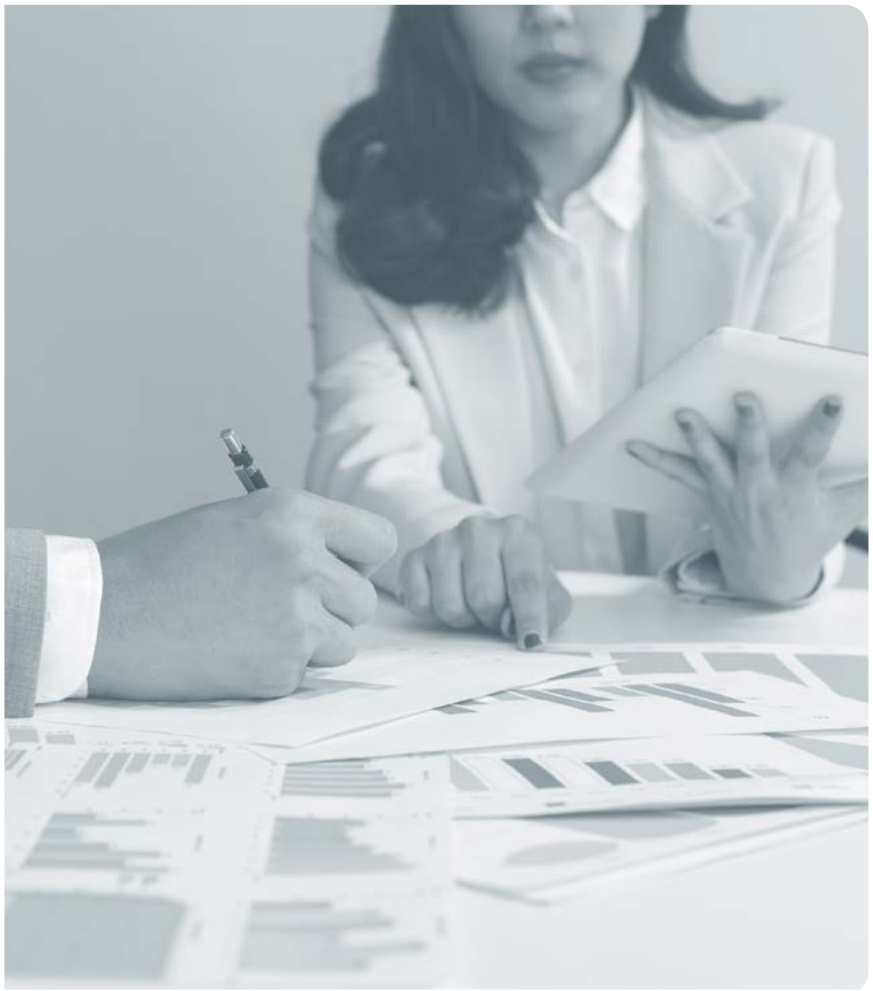
In an 1890 Harvard Law Review article — yes, 1890 — the authors coined the phrase "the right to be left alone" as a key tenet of privacy law. This definition of privacy was conceived for the analog world. Today, consumers are subject to unprecedented incursions to their privacy. The juxtaposition of big data, cloud computing, predictive analytics, and the Internet of Things enables organizations to collect and process vast amounts of information. Taken together, these create a digital fingerprint of behaviors that may expose personally identifiable information. There seems to be a sense of capitulation that in this digital age, privacy rights are destined to erode.

A recent Gartner report estimates that by 2020 the number of connected devices such as sensors and wearables will reach 21 billion, up from 6.4 billion in 2016. Such an unprecedented level of connectedness is expected to transform virtually every facet of our lives, largely in beneficial ways.

There are increasing concerns as to how the pervasive use of IoT devices will impact privacy rights. It's not just the volume of data generated, but also the variety of information collected, such as geolocation, internet search habits and preferences which, taken together, may infringe upon privacy rights.

Is obtaining informed consent practical when it comes to the world of IoT? There is an emerging school of thought that holds that the traditional consent model ought to be supplanted by a use model given that "ensuring individual control over personal data is not only an increasingly unattainable objective of data protection, but in many settings it is an undesirable one, as well."

We need new ways of thinking about the question of information stewardship. Stewardship has two components 1) a set of best practices — **what you do,** and 2) the character of the steward — **who you are**. We are learning that being cavalier — about who manages our data, what they do with it, whether the steward is in reality a potential competitor, and whether that steward also monetizes OUR data — has consequences.



DEVELOPED IN PARTNERSHIP WITH:

DOCAUTHORITY

DocAuthority

Organizations cannot leverage or secure sensitive information they cannot see, or they don't even know exists.

DocAuthority solves this problem through AI by discovering, automatically categorizing and accurately classifying secure sensitive files and documents with a patented high-value technology specifically designed to meet the data challenges facing businesses today.

For more information please visit us at
www.DocAuthority.com

LOOKING FOR YOUR NEXT STEP?

Do you have a question about this research? Would you like to discuss these findings with other members of AIIM?

CLICK HERE TO JOIN THE ONLINE DISCUSSION

CERTIFIED
INFORMATION
PROFESSIONAL

What's Next?

The CIP Can Help You and Your Organization Navigate the World of IIM.

Now is not the time to wait on your Digital Transformation initiative. IIM practices and methodologies are critical to your success, and AIIM can help. Digital disruption calls for digital leaders with the skills and experience to optimize information assets and transform business. Become that leader now through AIIM's Certified Information Professional (CIP) program.

AIIM worked with industry experts and focus groups to define the body of knowledge necessary for information professionals understand core IIM practice areas and methodologies, built a certification and test based upon this body of knowledge that is available at locations around the world, and created a set of training courses and materials to help information professionals prepare for the examination.

The path to CIP should be fairly simple for information practitioners who already have expertise and work experience. AIIM has a number of resources that can help practitioners at all levels prepare to become a Certified Information Professional:

- CIP Data Sheet
- CIP Exam Outline
- CIP Study Guide *(free to professional members; nonmember fee is $60 USD)*
- AIIM Training Courses
- Online CIP Prep Course
- In-Person CIP Prep Classes
- Practice Exam

CIPs reflect a more integrated, more holistic view of information management. Changes in one process, technology, or practice invariably affect others in the organization. CIPs are able to see the forest and the trees and understand and plan for these outcomes. Because of this, CIPs will identify and understand changes that could cause compliance issues, thereby reducing liability.

Organizations that manage their information more effectively enjoy reduced costs, faster time to market, increased revenues and cash flow, and increased business agility. CIPs are uniquely positioned to help organizations achieve these benefits because they understand the interactions between different information intensive processes and activities.

aiim

Here at AIIM, we believe that information is your most important asset and we want to teach you the skills to manage it. We've felt this way since 1943, back when this community was founded.

Sure, the technology has come a long way since then and the variety of information we're managing has changed a lot, but one tenet has remained constant. We've always focused on the intersection of people, processes, and information. We help organizations put information to work.

AIIM is a non-profit organization that provides independent research, training, and certification for information professionals.

AIIM
8403 Colesville Road, Suite 1100
Silver Spring, MD 20910, USA
+1 301 587 8202
www.aiim.org

AIIM Europe
Office 1, Broomhall Business Centre,
Worcester, WR5 2NT, UK
+44 (0)1905 727600
www.aiim.org