aiim InSights

Delivering the priorities and opinions of AIIM's 193,000 community


# GDPR Compliance: We're All Going To Be Fine(d)

In partnership with:

STAR STORAGE

aiim

# About the eBook

As the non-profit association dedicated to nurturing, growing and supporting the user and supplier communities of ECM (Enterprise Content Management) and Social Business Systems, AIIM is proud to provide this research at no charge. In this way the entire community can take full advantage of the education, thought-leadership and direction provided by our work. Our objective is to present the "wisdom of the crowds" based on our 193,000-strong community.

We are happy to extend free use of the materials in this report to end-user companies and to independent consultants, but not to suppliers of ECM systems, products and services, other than Star Storage and partners. Any use of this material must carry the attribution –
© AIIM 2017 www.aiim.org / © Star Storage 2017 www.star-storage.eu

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

Our ability to deliver such high-quality research is made possible by the financial support of our underwriting sponsor, without whom we would have to return to a paid subscription model. For that, we hope you will join us in thanking our underwriter for this support:

STAR STORAGE

8 Prof. Dimitrie Pompei Blvd,
Feper building, 1st floor,
Bucharest 020337, Romania
Phone: +4 (021) 242 13 95/96
Fax: +4 (021) 242 13 97
Email: products@star-storage.eu
www.star-storage.eu
www.seal-online.com

# About AIIM

*AIIM has been an advocate and supporter of information professionals for nearly 70 years. The association mission is to ensure that information professionals understand the current and future challenges of managing information assets in an era of social, mobile, cloud and big data. AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education, and certification programs to information professionals. AIIM represents the entire information management community: practitioners, technology suppliers, integrators, and consultants. AIIM runs a series of training programs, which can be found at http://www.aiim.org/Training.*

# About the Author

*Thomas LaMonte is an AIIM Market Intelligence Analyst, well versed and credentialed in the fields of ECM, ERM, and BPM with a heightened focus on solving the operational problems of today's businesses. Globally recognized as an industry thought leader, Thomas' opinions and views are highly sought after by business organizations of all sizes, from both the consumer and supplier communities.*

aiim

*Written by:*

Thomas LaMonte, Market Intelligence Analyst, AIIM Market Intelligence.

# Introduction

Less than 300 days separate us from the General Data Protection Regulation (GDPR) rollout in May 2018 in the European Union (EU). How well prepared is your organization to not only survive under these revised rules, but thrive in this data privacy minded new reality?

The intention of GDPR is to strengthen and unify data protection for all individuals within the EU, with an emphasis on personal data and sensitive personally identifiable information (PII). GDPR represents a big step forward for employee data privacy, granting greater control over the vast caches of personal information that proliferates in company databases, is shared across professional networks, and streamed via the internet to the world.

> "Less than 300 days separates the world from GDPR rollout in May 2018—are you prepared?"

Yes, the world!—the global aspect of GDPR is important to point out. So many businesses and services operate across borders, and therefore international consistency around data protection laws and rights is crucial both to organizations and to individuals. Although GDPR is a European regulation created to preside over the organizations physically residing in the European Union (EU)—and granted, the impact of GDPR is closest felt by businesses within the EU—its influence also stretches to any company transacting business within the EU domain. In short, GDPR has an international impact on the way businesses manage and protect their EU related information and data assets. All companies need to be aware of what is changing under the GDPR and prioritise efforts to prepare. With less than a year left to go before GDPR mandates go live, recent AIIM research finds that, on the ground, only 6% of companies report being fully prepared to meet GDPR requirements, and the indication is that the majority of companies are struggling to plan their compliance projects

Despite the challenges, at AIIM we believe GDPR is a good thing and improves data privacy for those that matter most—workers. If the GDPR is good for users, it's good for businesses. However, we also are aware of the

> "…only 6% of companies report being fully prepared to meet GDPR requirements…"

organizational challenges and pressures placed upon business owners and decision makers. For those of you in this type of leadership position—tasked with finding the best avenues to curtail GDPR risk and ensure that the business is up to GDPR code by next May—you may find yourself bombarded with recommendations and best practices, but which best practices are truly the best?

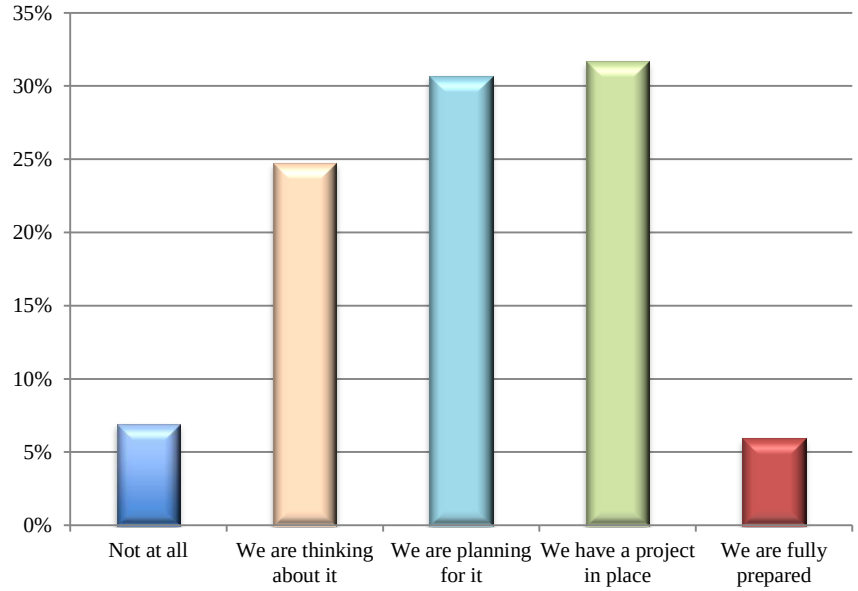
With fines as high as 20 million euros or 4% of total global turnover—whichever is greater—the stakes are high, and this isn't a time for a reactive approach to information governance and compliance.

To ensure that your countdown to GDPR ends in celebration rather than disaster, this eBook explores a proactive approach to GDPR, first with a primer on the current state of your peers' GDPR readiness, then an outline of new company responsibilities under GDPR regulations, and a crash course on the threat of noncompliance consequences. Finally, we conclude with steps to ensure GDPR compliance and how to build your own compliancy framework.

# Measuring GDPR Readiness

In the recent AIIM Industry Watch Report titled *GDPR: Understanding GDPR Readiness in 2017* (EU), we find that, as mentioned, only 6% of organizations voice that they are fully prepared to face GDPR. Thirty-two percent of respondents have GDPR projects in place to prepare for May 2018 enforcement, and 25% of respondents report that GDPR is on their company radars and they are thinking about it. (Figure 1)

**Figure 1: How would you rate the readiness of your organization in meeting GDPR requirements now?[1]**




Despite GDPR's inevitable arrival in less than 10 months, 7% of organizations have done nothing to prepare. AIIM senior analyst Bob Larrivee reflects on the dissonance gleaned from the AIIM GDPR Industry Watch Research, wondering what the root cause is that leads organizations to procrastinate or neglect GDPR preparation:

*"Considering there is still nearly a year to prepare, the combination of those who are "thinking about it" and those who feel they will have not done anything at all is quite significant and leads one to wonder if these businesses feel there is no real reason to be concerned, or if they simply do not understand GDPR and what the impact of noncompliance will be for them.[1]" AIIM Senior Analyst - Bob Larrivee*

What do you make of these findings? Is your organization ready for GDPR, and if not, why not? Do your company decision makers understand the gravity of its changes, or the impending threat on regulatory noncompliance? GDPR dispenses a brand new checklist of obligations, responsibilities, and regulatory changes that must be accounted for, and companies who want to stay competitive and avoid costly regulatory infractions must comply with GDPR changes moving forward. As we take a closer look into what this future under GDPR enforcement will look like, keep these questions in mind.

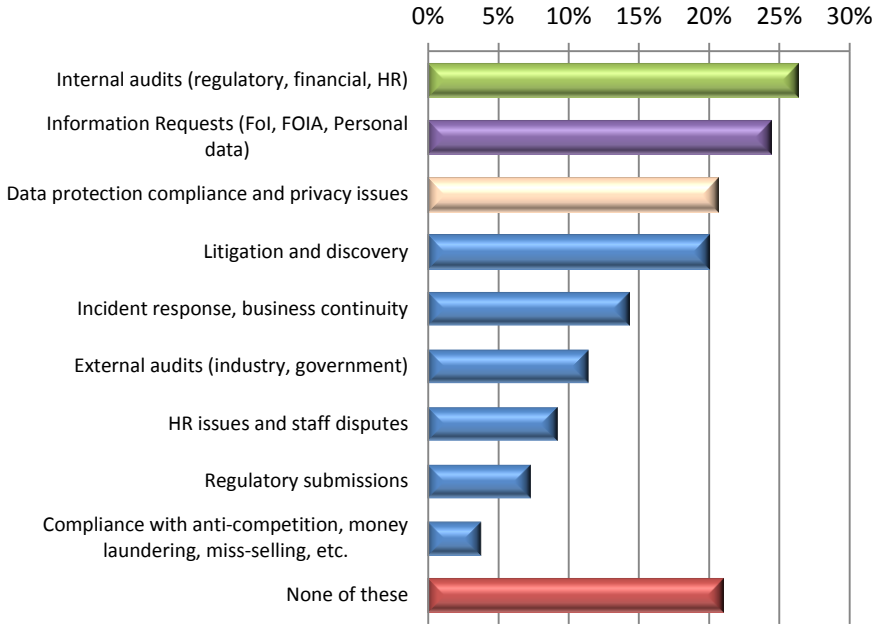
# *Is GDPR Really Going to Change Things?*

Yes, the implementation of the EU GDPR will require comprehensive changes to business practices for companies that had not implemented a comparable level of privacy before the regulation entered into force (especially non-European companies handling EU personal data).

This change is good: GDPR privacy protections and information governance reform come at an opportune time, as many organizations are suffering with compliance issues. When we asked the AIIM community if noncompliance despite good information governance practice causes significant issues, we found the following hardships as result of noncompliance:

- **26% experienced internal audit issues**
- **24% have had FOIA (Freedom of Information Act) or personal data request issues**
- **21% noted data protection challenges**
- **20% reported litigation and discovery problems**
- **Only 21% had no problems at all (Figure 2)**

**Figure 2: In your organization, has noncompliance with good Information Governance practice created a significant issue with any of the following in the last 2 years?[2]**




# Who and What is Affected?

The regulation applies if the data controller (organization that collects data from EU residents) or processor (organization that processes data on behalf of data controller, e.g., cloud service providers) or the data subject (person) is based in the EU. Furthermore, the regulation also applies to organizations based outside the European Union if they collect or process personal data of EU residents.

Hoping to get an estimate of the amount of organizations outside of the EU, and which would be affected— second-hand—by GDPR, we asked our community members to describe the ways in which their organizations based outside of the EU hold personal data on European employees and customers. Our poll takers revealed the following:

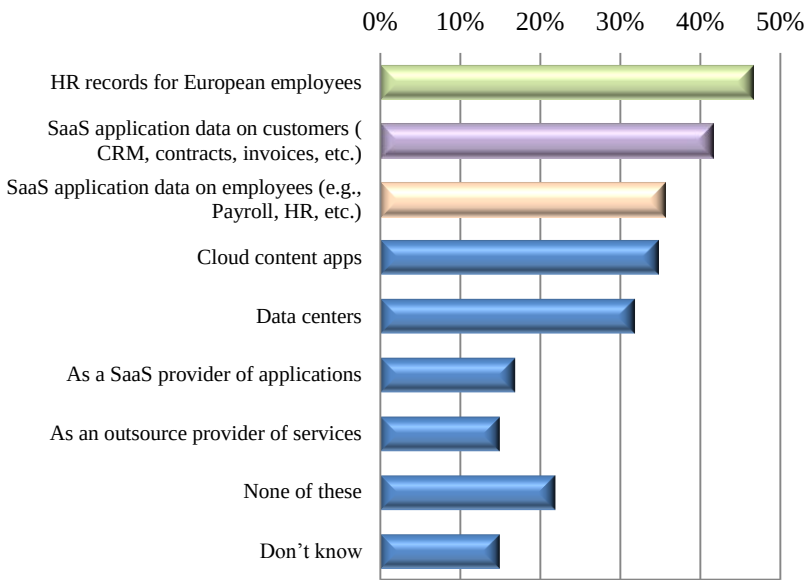
- **47% hold HR records for European employees**
- **42% are in possession of SaaS application data on customers (e.g., CRM, contracts, invoices etc.)**
- **36% retain SaaS application data on employees (e.g., Payroll, HR, etc.)**
- **35% maintain cloud content apps on behalf of European partners and customers**
- **32% host European company data centers (Figure 3)**

The "what" of this equation is information, more specifically, GDPR is about protecting personally identifiable information (PII). The concept of PII has been updated and includes two main components as defined by the European Commission:

1. "Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life."
2. "It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address.[4]"

What comprises PII has greatly extended under new GDPR definitions. Recalling the often quoted industry figure, 80% of information flowing through enterprises today is unstructured. Unstructured information is what we mean when we talk about information sprawl or information chaos, and includes email, paper documents, Microsoft office files, images, web pages etc, that are rapidly piling into our organizations en masse. As we can see, much of this type of content newly falls under GDPR jurisdiction, and organizations must be committed to building their enterprise networks with greater visibility and control over their sprawling unstructured information or face the consequences.

**Figure 3: In which of the following ways does your organization hold personal data on European employees and customers outside of your home region?[1]**




# What is My Company Accountable For?

1 **Privacy by Design and by Default:** requires that data protection is designed into the development of business processes for products and services. This requires that privacy settings must be set at a high level by default, and that technical and procedural measures should be taken care of by the controller in order to make sure that the processing, throughout the whole processing lifecycle, complies with the regulations. Controllers should also implement mechanisms to ensure that personal data is only processed when necessary for each specific purpose.[3]

2 **Consent:** Valid consent must be explicit for data collected and the purposes data is used for (Article 7; defined in Article 4).[4] Consent for children must be given by the child's parent or custodian, and verifiable (Article 8).[4] Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn.[3]

3 **Pseudonymisation:** The GDPR refers to pseudonymisation as a process that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information.[4] An example of pseudonymisation is encryption, which renders the original data unintelligible and the process cannot be reversed without access to the right decryption key. The GDPR requires that this additional information (such as the decryption key) be kept separately from the pseudonymised data. Pseudonymisation is recommended to reduce the risks to the concerned data subjects and also help controllers and processors to meet their data-protection obligations (Recital 28).[3]

4 **Right to Erasure:** A right to be forgotten was replaced by a more limited right to erasure in the version of the GDPR adopted by the European Parliament in March 2014. Article 17 provides that the data subject has the right to request erasure of personal data related to them on any one of a number of grounds; this includes noncompliance with article 6.1 (lawfulness), which carries case (f) where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.[3]

5 **Data Portability**: A person shall be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller. In addition, the data must be provided by the controller in a structured and commonly used electronic format.[3]

# What are the Sanctions for Noncompliance?

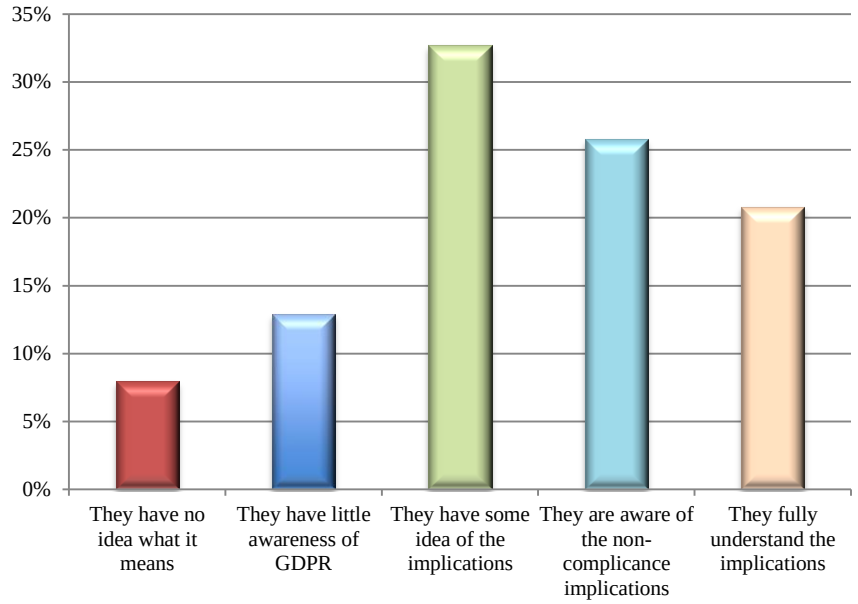
GDPR noncompliance ramps up consequences with a climax of business crippling fines:

- **A warning in writing in cases of first and non-intentional noncompliance.**
- **Regular periodic data protection audits.**
- **A fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.**
- **A fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.**

Lack of understanding GDPR infractions will not be a valid excuse come May 2018. Noncompliance is costly and organizations must be ready. New technology and of course new roles and recruitments are emerging; beyond IT and technology upgrades, investment in privacy personnel, employee training, and data policies will be mandatory. Some companies will also find it valuable to appoint specialized data protection officers (DPO) to help mitigate the potential threat of GDPR noncompliance. A number of organizations are course correcting, and solutions are available, but recent data is troubling: only 21% of our respondents say that their organization's executives fully understand the implications of GDPR noncompliance, and an equal 21% confess that their senior employees have little or no understanding of what GDPR noncompliance means for their organizations. (Figure 4)

It seems a significant number of companies suffer an education problem, most fatally one presiding at the top of the management pecking order, which suggests a second problem: resistance to change. To avoid collision with GDPR in May, organizations need to find a way to ensure all staff members, top-to-bottom, are aligned in their understanding of GDPR and the urgency for compliance as well as the benefits.

**Figure 4: How would you rate the level of understanding your executives have of the implications of GDPR noncompliance?[1]**




# Closing Thoughts

GDPR is the driving force to move businesses toward stronger data protection practices, but it should be seen as a positive motivator and an opportunity to do what must be done—and should have been done all along. It is also an opportunity to evaluate how technology will support your information governance (IG) initiatives and align your business to comply with GDPR to strengthen your practices, identify weakness, and begin to close the gaps. Decisions makers need to be asking themselves key questions: are your organization's current information management technology solutions doing enough? What about your current vendor's roadmap—are you satisfied? Are vendor upgrades aligned with and moving in the same direction as your company plans for data security and compliance assurances, emerging tech

like cloud and mobile access, and strategies to integrate core systems and core goals—including GDPR compliance? Perhaps it's time to look at new options?

It's also important to realize that GDPR is just the beginning. Senior Vice President of AIIM, Atle Skjekkeland, posits an innovative vision for the future:

> "*Today, we are living in a period of transformation. There are traditional players in this space but also new generation solutions, innovation, a new approach in business content services and information governance.*" *AIIM Senior Vice President – Atle Skjekkeland*

Along with new ideas, methods, and disrupters, in this new world of information management, according to Atle *Skjekkeland*, user experiences—(line of business users, not IT) will take center stage and "really matter." Atle continues: "*Powerful capabilities "hidden" in a simple to use interface is key for real usage."*

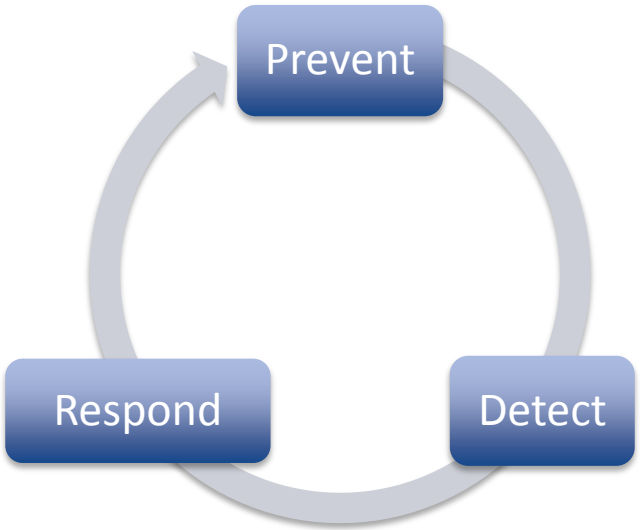
GDPR is a mile marker for more innovative times, technology, and strategies to manage our information assets. Adjusting to GDPR mandates is part of the much bigger story of intelligent information management. Recalibrating process, technology, and people to comply with GDPR is the first hurdle, but the real challenge will be to ensure that change takes anchor in our corporate cultures. GDPR compliance is not just about the Chief Compliance Officers, Legal Directors and Chief Security Officers – it is about all the line of business users doing their job every day. GDPR is about people, and if we commit to supporting the information needs of people, we're all going to be fine.

# Proactive Steps to GDPR Compliance

To best aid your efforts to prepare for the GDPR here are eight recommendations to lead your organization to successful GDPR compliance, and prepare for a new reality of intelligent information management:

- Identify use of personal data and content to ensure lawfulness, fairness, and transparency.
- Limit purpose and data minimization by only collecting information for specified, explicit and legitimate purposes.
- Connect data and content to get a unified view for better control, portability, and deletion.
- Use metadata to ensure privacy-by-design and by default compliance.
- Apply retention management to limit storage requirements.
- Use encryption at transit and at rest to ensure integrity and confidentiality.
- Use access control lists, permission management, and audit trails to ensure compliance.[3]
- Establish a Compliancy Framework.

# Establish a Compliancy Framework:




## 1 Prevent

- Risk assessments
- Training
- Policies & procedures
- Executive commitment
- Deploy Systems easy to operate by LOB users

## 2 Detect

- Data Protection Officer
- Audit
- Monitoring

## 3 Respond

- Reporting
- Investigation
- Communication
- Improvements
- Employee discipline

## References

[1]*AIIM Industry Watch Report titled – "Understanding GDPR Readiness in 2017"*

[2]*AIIM Industry Watch Report titled – "Information Governance: too important to be left to humans"*

[3]*AIIM Keynote Speaker Atle Skjekkeland, SVP – "GDPR: How to Ensure Compliance"*

[4]*General Data Protection Regulation (GDPR) – https://gdpr-info.eu*

## UNDERWRITTEN BY

Star Storage is a global technology provider developing and delivering state-of-the-art information protection and management solutions for top private and public organizations. With more than 17 years of experience, own Intellectual Property and a portfolio of over 500 customers on 4 continents, strong expertise in top industries such as banking, insurance, telecom, manufacturing, utilities and public administration, the company plays a key role in the digital transformation, mobile and cloud journey of any size organization.

8 Prof. Dimitrie Pompei Blvd, Feper building, 1st floor,
Bucharest 020337, Romania
Phone: +4 (021) 242 13 95/96
Fax: +4 (021) 242 13 97
Email: products@star-storage.eu
www.star-storage.eu

AIIM (www.aiim.org) is the global community of information professionals. We provide the education, research and certification that information professionals need to manage and share information assets in an era of mobile, social, cloud and big data.

Founded in 1943, AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education and certification programs to information professionals. AIIM represents the entire information management community, with programs and content for practitioners, technology suppliers, integrators and consultants.


AIIM
1100 Wayne Avenue, Suite 110
Silver Spring, MD 2091
(+1) 301 587-820
www.aiim.org

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