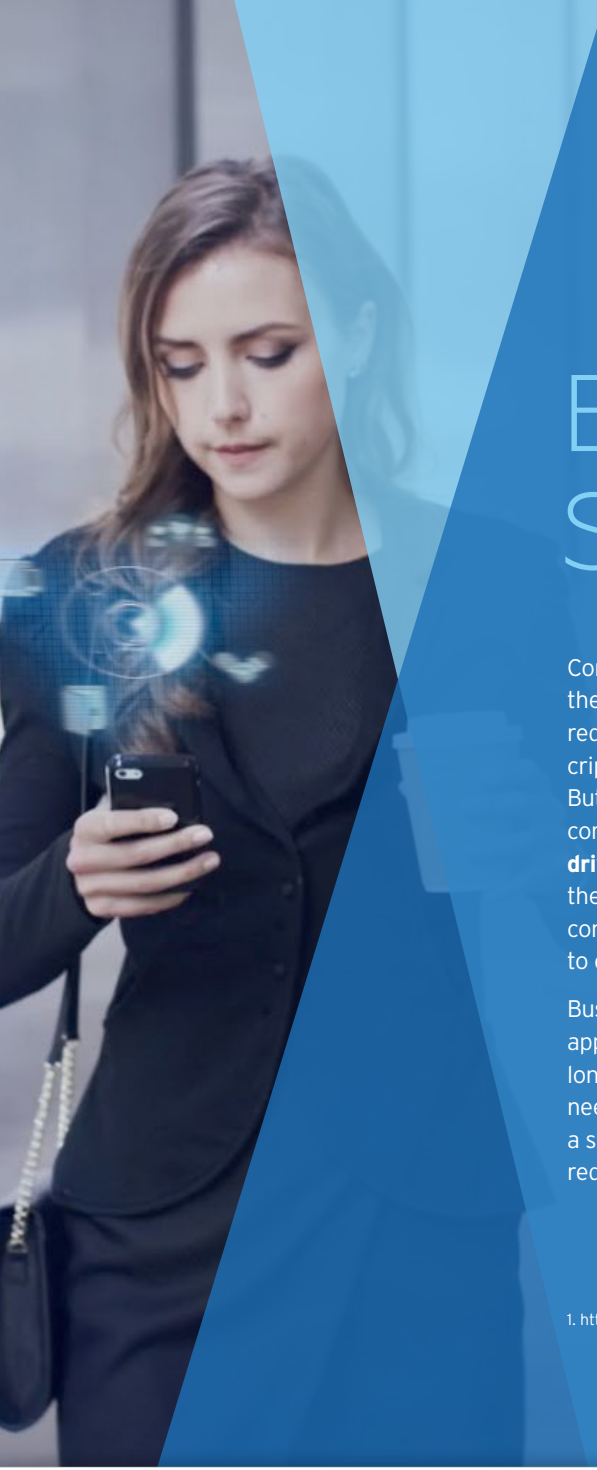
SETTING SAIL TOWARDS COMPLIANCE

Navigating the challenges of compliance in a privacy-first world

IRON MOUNTAIN®



EXECUTIVE SUMMARY

Compliance. Privacy. GDPR. All too often do these words evoke images of mountains of red tape compounding in the prevailing fear of crippling fines for failing to meet their demands. But things are changing. No longer is achieving compliance all about ticking boxes; it's about **driving a culture change** in an era where the trust deficit is one of the biggest societal concerns of all. It's an opportunity for businesses to earn back the trust of their target audiences.

Businesses have traditionally taken a reactive approach to compliance[1]. The top concern has long been to minimise the time and investment needed to be able to prove to regulators that a specific rule has been met. With regulatory requirements being generated on a global, national, and even a local level, the demands aren't getting any easier to meet. Just 'getting it done' is no longer practical, or even desirable. Instead, it requires a strategy that starts with the very foundations of modern business operations. It demands **privacy by design and default**.

But let's take a more positive outlook. Navigating the new information landscape and enabling privacy and security by design and default isn't just about staying on the right side of the law. It's also the only way today's organisations can:

- Ensure business continuity
- Empower innovation without adding risk
- Turn trust into a value proposition
- Derive greater insights from data
- Meet the challenges of scale

1. https://www.complianceweek.com/best-practices-in-policy-management/2218.article

CHAPTERS IN THIS GUIDE:

1 PRIVACY BY DESIGN: A MODEL OF PREVENTION

2 TURNING COMPLIANCE INTO A COMPETITIVE ADVANTAGE

3 EVALUATING THE FUNDAMENTALS OF GOOD INFORMATION MANAGEMENT

"Privacy by design and default raises the bar on privacy dramatically, because what it says to customers is that they don't have to ask for privacy – it's given to them automatically."

Ann Cavoukian, Founder of Global Privacy and Security by Design Centre

In the age of social media, it's easy to assume that people are willing to share their lives online, even if that means surrendering their private information to the businesses which provide them the means to stay connected. As such, **consumer privacy** has largely revolved around lengthy policies which people rarely read in full. As soon as a user checked the obligatory box stating they agree with said policy, that's where compliance began and ended. Only afterwards do the privacy-invasive events manifest themselves, which is usually about the time when the user realises they've unwittingly yielded their private data for a multitude of purposes, such as advertising, that they might not have thought about before.

It's safe to say that the damage has already been done by that stage. Consider, for example, how difficult it is to delete your Facebook account; a process which doesn't typically become permanent for a few weeks. This is partly due to the interconnectivity Facebook, and many platforms like it, have with other online services, some of which use them for identification and login. Many companies have a clear strategy for locking people into broader ecosystems. In other words, **privacy is defined by a policy that hardly anyone reads**, while the risks and the steps needed to mitigate them only become fully apparent later on.

That's a good example of how not to do things in a privacy-first world where GDPR and similar regulations strive to give back control to the end user. While regulatory compliance is typically seen as something that comes after the event, new rules revolve around **proactive measures** that give end users the chance to **explicitly grant permission** to businesses wanting to collect and use their information. This is one of the core principles of privacy by design.

PRIVACY BY DESIGN: A MODEL OF PREVENTION

1

Instead of waiting for privacy risks to materialise, the concepts of privacy by design are baked into the code of every application and included in the foundations of every business process. Since people generally rely on technology to make their lives simpler, they're also more likely to accept the default settings if only to save time. That's why **privacy must also be the default setting.** In other words, if an individual does nothing, their privacy is still protected. Only when they decide they want to access a function or feature which *requires* them to allow access to their private information, must they explicitly provide permission. Consider, for example, how you need to grant permission for a photo-taking app access to your device's camera. It's a user-centric approach that keeps people informed throughout the lifecycle of the data involved.

Recap of the foundational principles of privacy by design

Privacy must:

- be proactive and preventative, not reactive and remedial
- always be the default setting
- be embedded into the design of every app and process
- not come with any unnecessary trade-offs
- extend to the full lifecycle of the data involved
- ensure all operations remain visible and transparent
- put the interests of the individual, not the business, first

CHECK ICO'S DIRECTION ▷

TURNING COMPLIANCE INTO A COMPETITIVE ADVANTAGE

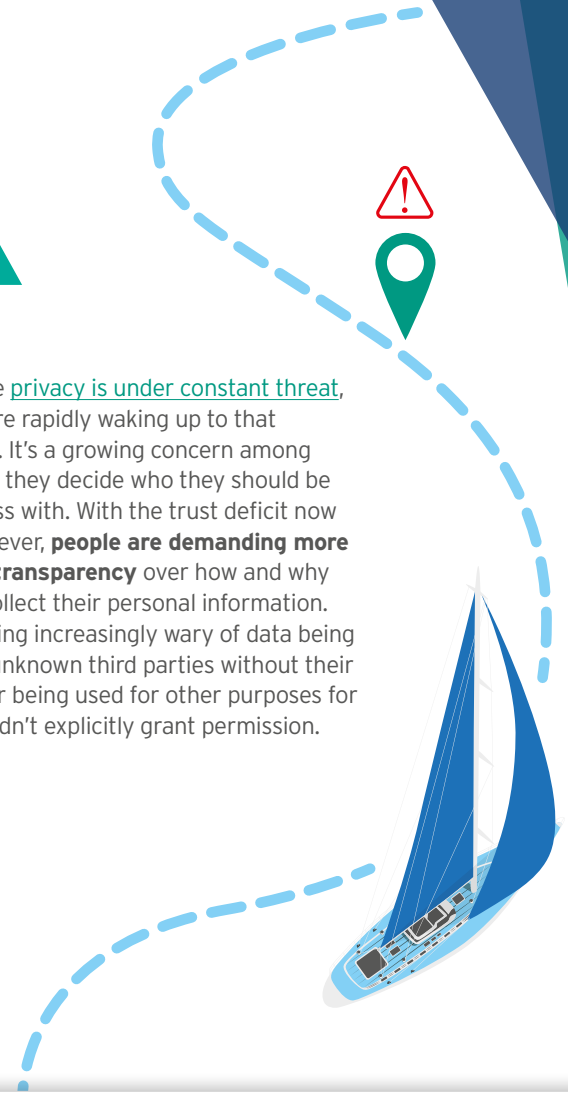
2

"Businesses can gain a competitive advantage by proactively embedding privacy into their operations so that, not only will business interests win; they'll build a trusted relationship with their customers"

Ann Cavoukian, Founder of Global Privacy and Security by Design Centre

Compliance has traditionally been viewed in a rather negative light in the business world. Many leaders see it as a bureaucratic hurdle, a blocker of innovation, or a necessary evil. After all, it's rarely easy to achieve compliance, which is why many enterprises have fallen behind when it comes to meeting their obligations. For example, one recent report found that little over a quarter of companies had successfully achieved full GDPR compliance even 17 months after the law came into force[2]. But, despite such a disappointing statistic, **81% of companies which declared themselves to be fully compliant had reported positive impacts on brand reputation**. In other words, compliance isn't a hurdle; it's a driver of business.

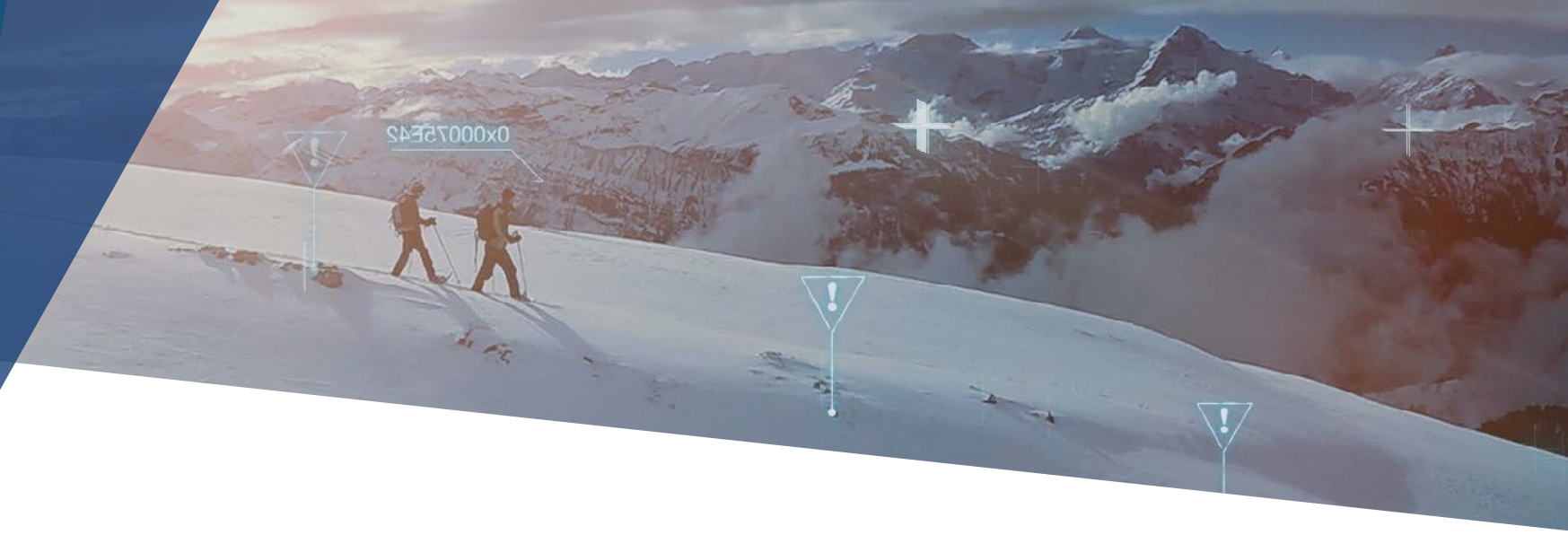
Talking about **compliance as a competitive advantage** might sound like an oxymoron, but it's now clearer than ever that the two are directly related. After all, we live in a surveillance culture where privacy is under constant threat, and people are rapidly waking up to that sobering fact. It's a growing concern among customers as they decide who they should be doing business with. With the trust deficit now greater than ever, **people are demanding more control and transparency** over how and why companies collect their personal information. They're growing increasingly wary of data being shared with unknown third parties without their knowledge, or being used for other purposes for which they didn't explicitly grant permission.



2. https://www.capgemini.com/news/data-protection-and-privacy-report

TURNING COMPLIANCE INTO A COMPETITIVE ADVANTAGE

2



YouTube had to pay

$170m

for violating the Children's Online Privacy Protection Act (COPPA)[3]

For too long, many among the business world have taken a **zero-sum approach** to privacy, in which there's a widespread belief that putting the control back in the hands of customers is bad for business. In other words, the supposed business interests end up coming first, when they should actually be secondary to privacy. That's because achieving privacy is itself now a business interest; a big plus as far as customers evaluating companies are concerned. Now that anyone can head to Trustpilot and other review platforms to vent their frustrations with businesses which don't respect their privacy, the role of privacy by design in achieving a good brand reputation should be obvious.

To **build trusted business relationships**, companies need to **take a positive-sum approach** to the way they collect and use consumer information. In other words, it needs to be a win-win for both parties in the transaction. By being upfront about their data-collection processes, they can win more business. For example, if the opportunity of a secondary use for data arises later on, after it's been collected, businesses can return to their customers and seek their consent. Most of the time, **people will appreciate the transparency** and willingly give their permission, thereby solidifying the relationship and driving innovation and prosperity on both sides. If, on the other hand, the business just does whatever it wants with the data without permission, it's a breach of trust and compliance alike. That can lead to a severely tarnished reputation and a large fine.

To summarise, embedding privacy by design and default into every business function doesn't just protect your reputation; it's a fundamental part of your value proposition that helps your business thrive in a **privacy-first world**.

3. https://www.theverge.com/2019/9/4/20848949

"The volume and format of data, particularly when there's a lot of physical media involved, combined with the need to gather all of it within limited timeframes, presents a huge challenge for businesses"

Michael Zurcher, Global Privacy Officer at Iron Mountain

Overcoming the practical implications of implementing privacy by design is undoubtedly the greatest challenge organisations face, particularly if they've been collecting data over multiple decades in dozens of different formats. Given the **fast pace of technological** development, the problem becomes exponentially harder to tackle the longer the company has been in business and the more past and present customers it has. Indeed, the sheer volume of data generated by everyday business operations has far outpaced the capabilities of many companies to keep up. One recent study found that less than a third of organisations consider themselves to be data-driven[4], despite the fact they're collecting more data than ever.

In the end, **it all comes down to good information management**. With the right processes in place, business leaders can derive greater insights from data and empower innovation without adding risk. Every sufficiently robust information governance programme should follow certain principles to ensure it's ready to tackle the challenges of compliance and security both today and tomorrow.

Less than

1/3

of organisations consider themselves to be data-driven

4. https://hbr.org/2019/02/companies-are-failing-in-their-efforts-to-become-data-driven

EVALUATING THE FUNDAMENTALS OF GOOD INFORMATION MANAGEMENT

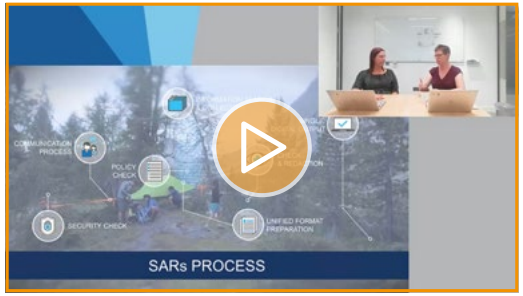
3

10 steps to setting up a future-proof information governance programme

1. Educate all employees on their roles and duties to protect information per the terms of your compliance and security policies.
2. Confirm the authenticity and integrity of information and eliminate any inconsistencies.
3. Store all information in a unified, enterprise-approved record-keeping repository.
4. Classify information under the correct record code to ensure necessary compliance and security controls are applied.
5. Prevent the unnecessary proliferation of information with measures like data loss prevention and zero-trust access controls.
6. Dispose of information securely once it reaches the end of its lifecycle and no longer has legal or operational usefulness.
7. Secure all confidential customer and enterprise information at rest and in transit with encryption and multifactor authentication.
8. Comply with subject access requests (SARs) by responding within 30 calendar days (in the case of GDPR).
9. Align all business systems and processes with information governance standards from the moment they're implemented.
10. Ensure third parties with access to customer or business information are also in compliance with your governance standards.

Step 8 – **complying with SARs** – has proven a tricky one for many companies. When making a request, the individual has the right to ask which information is being processed, what type of data it is, why the company has it, and how it was collected. Companies may also be asked to provide evidence of how it is being safeguarded. All SARs must be responded to within 30 calendar days. Responding to SARs within the legally mandated timeframe can be extremely difficult, since information often exists in unstructured formats, such as paper documents and email archives. Some enterprises even still have information stored on long-obsolete formats like microfilm. Naturally, such information isn't easily searchable like that stored in an industry-standard database format. The degradation of physical media can also present problems.

DOWNLOAD SARS CHECKLIST ▷



Overcoming these challenges now and tomorrow means that businesses need to migrate to a **cohesive information-management environment** where the process is largely automated. It's time for businesses to get a handle on information overabundance and delete what they don't need and ensure their policies are up to date. They need an information lifecycle management routine which can do that automatically. Fortunately, there are many ways new technologies can help. For example, **optical character recognition (OCR)** can digitise paper documents to make them searchable, while **artificial intelligence (AI)** can make sense of large amounts of unstructured data. Together, these solutions help you migrate to a more scalable and manageable infrastructure, which adds value to every business process.

LAYING THE FOUNDATIONS FOR INNOVATION WITHOUT THE RISK

No one's suggesting that implementing privacy by design is easy, especially for established organisations and platforms, which often have to rework numerous business processes and systems to become compliant. But privacy is also a **fundamental human right** in a time when it faces constant assault from unscrupulous advertisers. Fortunately, there are many ways privacy by design can add value throughout the business.

Embedding privacy by design inherently requires a more cohesive and efficient information-management ecosystem, one which will **help your business become more data-driven**.

Achieving compliance drives **stronger business relationships** in a time when consumers are increasingly wary about who they do business with.

With the right information-management processes in place, businesses can **become more scalable and adaptable** to both current and future demands of regulatory compliance.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organisations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centres, art storage and logistics, and cloud services, Iron Mountain helps organisations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.co.uk for more information.

08445 60 70 80 | IRONMOUNTAIN.CO.UK
R.O.I. 1800 732 673 | N.I. 08445 60 70 80 | IRONMOUNTAIN.IE

IRON MOUNTAIN®