

7 Tips for GDPR Compliance

Practical strategies for meeting compliance requirements



Downloading

Executive Summary

Much has been written about the European Union's (EU) General Data Protection Regulation (GDPR), which comes into effect on May 28, 2018. The law impacts any company that processes the personal data of EU citizens, in terms of what they do with it and how they store it. While most organizations have an awareness of what the law covers, there's much less clarity over how to actually implement its requirements.

This whitepaper takes the position that for many organizations, ensuring compliance with the GDPR will largely come down to good information governance processes. We focus particularly on how simple changes in the way businesses store and manage the information they collect will go a long way to giving them the peace of mind that they are in line with the new legislation.



Contents

- 04** | The GDPR is the push information governance has needed
- 06** | GDPR overview
- 08** | How does the GDPR affect information governance?
- 10** | Seven practical actions for implementing information governance to ensure GDPR compliance
- 16** | The last mile in GDPR compliance
- 18** | Peace of mind knowing you are GDPR compliant




“ **GDPR will largely come down to good information governance processes** ”

The GDPR is the push information governance has needed

The past two decades have seen a surge in the amount of data that companies of all sizes collect about their customers. Digital technologies make it significantly easier to capture details about a business' customers and also analyze that data to build a more intimate profile of the spending habits and lifestyles of their customers.

Businesses are regularly exhorted¹ by industry thought leaders to utilize the data they collect about their customers. It can help them discover buying trends, decide on special offers, or create personalized marketing messages which will make customers more likely to spend their money.

In theory, this is fine. However, many organizations have proven they are less than satisfactory at managing the balance between collecting customer data and ensuring it is managed securely:



Countless data breaches, at companies as diverse as eBay, Adult Friend Finder and Target, have resulted in leaks of personal information into the public domain, to the embarrassment of customers.²

Consumers have become increasingly uncomfortable with companies collecting their personal information, and trust in even major digital brands such as Apple and Twitter is now relatively low.³

Support for 'reigning in' many of the world's biggest technology companies is growing, with a perception that they are becoming too powerful and are building monopolies.

Many existing privacy laws are simply irrelevant to the digital era where consumers leave a trail of personal and intimate data whenever they connect to the internet.

¹ Smart Insights, 2016. Why Customer Data Should Shape your Marketing Strategy. Available online: <https://www.smartinsights.com/customer-engagement/customer-engagement-strategy/customer-data-shape-marketing-strategy/>

² CSO Online, 2017. The 16 biggest data breaches of the 21st century. Available online: <https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html>

³ The Verge, 2017. The Verge Tech Survey. Available online: <https://www.theverge.com/2017/10/27/16550640/verge-tech-survey-amazon-facebook-google-twitter-popularity>

This combination of factors has pushed the EU to take a tough regulatory stance regarding how businesses collect and process customer data in the digital era, resulting in the GDPR.

However, many companies continue to struggle with governing the data they collect about their customers. Their processes and policies for managing data are insufficient, often disorganized and poorly managed. This increases the chances of data breaches occurring, and once the GDPR comes into effect, sanctions against firms that fail information governance

audits will be severe (**€20 million or 4% of annual global turnover – whichever is higher⁴**).

Providing your organization processes the personal data of EU citizens, regardless of where you are based, you will almost certainly be affected by the GDPR.

This [whitepaper](#) will therefore provide you with concrete information management steps you can take to become compliant, while also improving how your organization collects and manages data.

GDPR maximum penalties

€20 million or 4% of annual global turnover – whichever is higher.

Deadline

25th May 2018 - the date on which the GDPR comes into effect.

Brexit

British companies will be affected until Brexit actually happens in 2019, and most will still be affected beyond that.

⁴ EU GDPR, 2017, GDPR Key Changes. Available Online: <https://www.eugdpr.org/key-changes.html>

GDPR

Overview

The GDPR is a wide-ranging privacy law which covers a broad range of activities. Some of its most significant factors include:

- Any company that collects private data on EU citizens is affected – regardless of where it is based. The GDPR will allow the EU to prosecute any company in the world which processes the data of EU citizens but fails to comply with the GDPR.
- Almost any private customer data comes under the purview of the law – from the individual's name to their email and IP address, religion, ethnicity or location.
- Businesses will have to gain explicit consent from customers each time they collect and use their data.
- Larger businesses, with over 250 employees, will have to appoint an independent data protection officer (DPO). The new role is also recommended for smaller firms that process large quantities of personal data.
- Anyone intending to do anything new with personal data that has already been collected (such as attempting to connect data from a loyalty card program with their customers' online activity for customer profiling) will have to complete a 'privacy impact assessment'.
- Any time a data breach happens, companies will be required to report it to the relevant authorities in their country within 72 hours of discovering the breach.
- The so-called 'right to be forgotten' will allow consumers to demand that any information a company holds on them be erased. The law also prohibits the data from being used for any purpose other than the one it was originally collected for – unless further consent is gained.
- Privacy by design is now expected in any systems or data processing tool that organizations use.



What counts as 'personal data'?

Article 4 of the GDPR states:

“Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’)... An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”⁵

⁵ GDPR Info, 2017, Article 4, GDPR Definition, Available online: <https://gdpr-info.eu/art-4-gdpr/>



How does the GDPR affect information governance?

At present, information governance laws vary across the EU. Some countries, such as Germany and Spain, already have strict laws which prohibit the movement of private data outside national borders, for instance. Other countries, such as Ireland, have traditionally offered a more relaxed regime. However, when the GDPR comes into effect, the way businesses collect and manage information will change significantly, and they will need to move towards much stricter models.


Most organizations today will follow their own data and information management policies, where access to the environment will require a password. These environments will typically incorporate:

- Permissions levels
- Rules on what kinds of information to store and where
- Policies on who accesses data and what they can do with it

By and large, most environments of this kind – such as SharePoint, Office 365, Salesforce or Dropbox – provide the levels of security and privacy which businesses will need to comply with the GDPR. They make it easy to search for information, delete personal files if a customer requests it, and usually have strong defenses against external breaches.

However, the limitation is that all too often, business users do not follow their organization's information governance policies. Whether it's because storing content in these platforms is onerous, or simply ignorance of the rules, customer data can end up being used in a way which violates the customer's privacy and the GDPR's rules.

Compliance with the GDPR will therefore require practical steps which both improve employee awareness and the practices which make it more likely people will follow the rules.



Employees could easily violate the terms of the GDPR

There are many seemingly innocent ways that business users could unintentionally violate the GDPR:

- A hiring manager for a controversial energy company meets a candidate in a restaurant to discuss a new role, and asks to record the conversation on her personal smartphone to save taking written notes. Later, her smartphone is attacked by hacktivists who publish the recording on a website.
- A housing tenant shares personal information, such as their salary, address, age and gender with an estate agent via email. The email is never stored in a secure environment, and instead remains in the agent's inbox. Months later, when the agent has left the company, the tenant requests all information the agency has on her, but none can be found on the central system because the agent never moved it there from his inbox.
- A boutique fashion house has been acquired by a major conglomerate. The marketing manager at the conglomerate wants to discover if there are any customer cross-overs between the parent firm and the boutique company, and begins crunching through email addresses and customer data to compile a marketing email list and begins sending customers special offers. However, since this would require using the data for a different purpose for which it was originally shared, the company would be in violation of the GDPR.

7 practical actions for implementing information governance to ensure GDPR compliance

In many ways, GDPR compliance can be achieved by following best practice for information governance and a strict policy which all employees follow. The following seven actions can be implemented rapidly in most organizations and will immediately improve your ability to be GDPR compliant.

1

Explicit consent when collecting any personal data

One of the GDPR's main concerns is that businesses are collecting ever more data about consumers and the general public without providing them with information about what they are doing and why. To use many services – from health and fitness apps to insurance contracts to online checkouts – users are obliged to provide personal data, yet companies offer little transparency. The GDPR aims either to limit this, or to force companies to be upfront about why they are collecting the data.

Actions to take:

- Create a generic legal document you share with customers whenever you collect their personal data, explaining what you do with their data and why you are collecting it. Allow them to opt out of anything but the essentials if they so wish.
- Limit the amount of data you collect – many companies collect data just in case it will be useful in the future. This goes against the spirit of the GDPR; if you don't have a specific reason for knowing someone's telephone number, their sexual orientation or their ethnicity, simply stop collecting such information.
- If you plan to do anything with the customer's data (such as performing background checks), you must now explain exactly what you will do with it.
- Train staff who collect customer data in their role about what the GDPR means. Whether you're an insurance firm or a recruiter, a healthcare company or a sports equipment provider, you need your frontline staff to understand that there will be changes in information you collect about customers.

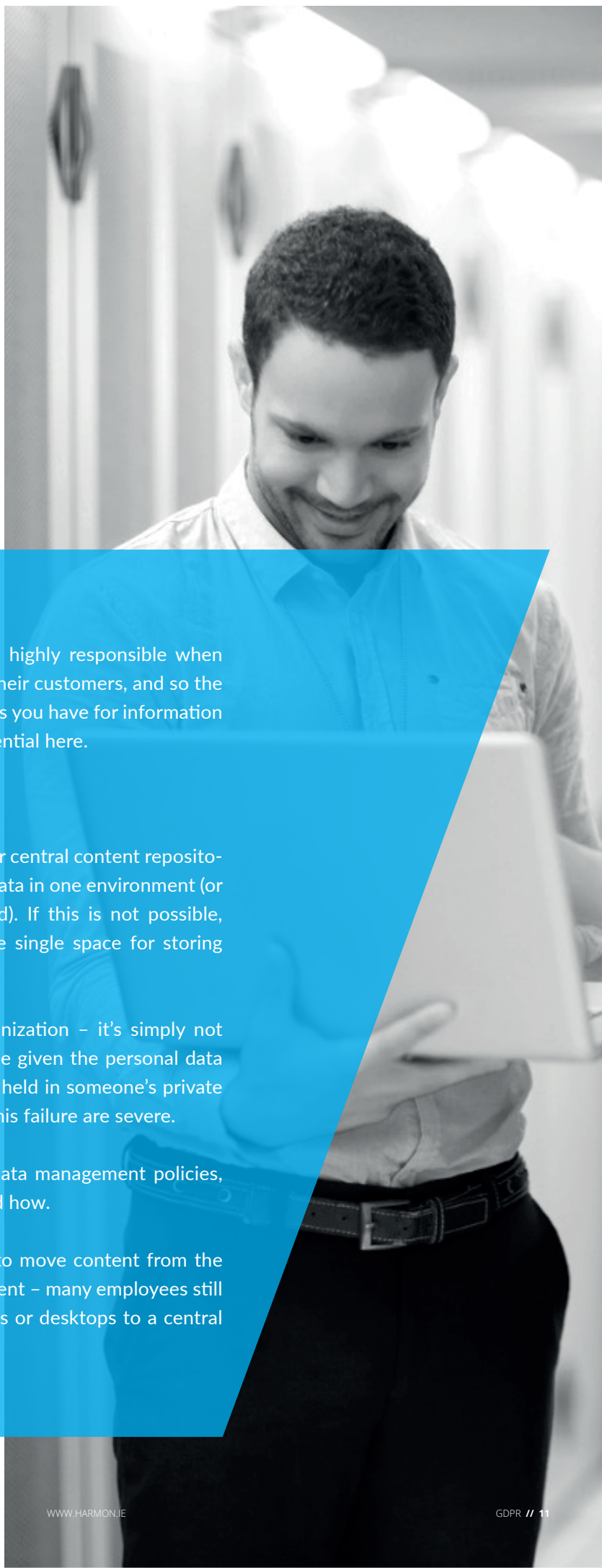
2

Choosing how to store

The GDPR expects organizations to be highly responsible when storing any personal information about their customers, and so the technology you use, as well as the policies you have for information governance and user training, are all essential here.

Actions to take:

- As far as possible, you should unify your central content repository. Aim to store all personal customer data in one environment (or connect on-premises and/or the cloud). If this is not possible, make sure that departments have one single space for storing data.
- Eliminate any shadow IT at your organization – it's simply not worth the risk. If a customer asks to be given the personal data you hold on them, and it turns out it's held in someone's private Dropbox account, the implications of this failure are severe.
- Train staff, or refresh them, on your data management policies, reinforcing where content is stored and how.
- Make it as easy as possible for users to move content from the tools they use to your secure environment – many employees still fail to move content from their inboxes or desktops to a central location.



3

Audit what information you hold

One of the easiest ways to begin complying with the GDPR is to perform an audit of all the information you currently hold, and search for any personally identifiable information (PII) that may exist across your organization. Collect this data and make decisions about what you want to do with it.

Actions to take:

- Perform an audit of all your IT systems and content management platforms to find PII.
- Move any data you still wish to keep to a centralized and secure environment.
- Delete any data which no longer offers any real value to your business, including historical customer data. If the data no longer exists, you are no longer responsible for it.



4

Make subject access information easier to find

One of the major features of the GDPR is that it gives more power to the consumer. As of May 2018, consumers will have the right to demand a 'subject access request', where you must be able to provide them with a file containing all the information you hold on them. To be compliant, you will need to confidently collect data from all your systems about a specific customer, which may involve collating data from multiple systems, such as your SharePoint, CRM, employee inboxes and any backend data processing systems.

Actions to take:

- Train staff on the importance of storing PII in your internal content platform. Employees must be made aware of the importance of moving all communications with clients that involve personal information to somewhere it can be found later.
- Deploy technology which allows you to search across the environments you use to store customer data – whether it's SharePoint, Salesforce, Email, ZenDesk or something else.
- You may find it valuable to give one employee the specific responsibility of compiling subject access requests. They can compile a checklist of places to search for content, and build a template document for presenting this information in a comprehensible way (rather than meaningless rows of data in a spreadsheet, for instance).



5

Privacy by design

The GDPR expects that any technologies you use to collect customer data will focus on protecting that data first. If your company offers a smartphone app or web tool – be that an insurance quote generator, a health and fitness monitor or an education tool – you will need to review everything about how the app works in order to ensure it is safe and secure. Even companies that do not have this kind of app, must store any data they collect via internal systems, in a secure platform.

Actions to take:

- Review any apps you have which currently collect customer data and secure these with encryption and password protection.
- Carry out an assessment of your current cybersecurity defenses and processes. Are there any weak points in your systems, any staff still carrying key data on unprotected USB sticks, for instance?
- Promote simple best practice steps – such as ensuring people move any customer PII from email to a secure records management folder.



6

Accountable records management processes

The GDPR means your customer records management process must be secure throughout its lifecycle. Whether you're an accountant for small businesses, a real estate agent or a healthcare provider, any personal customer information that your staff receives must be recorded centrally, have permissions and metadata tags applied, and you must move those records through their storage process to efficient destruction when no longer required.

Actions to take:

- As far as possible, avoid the use of paper records in your processes.
- Train staff on the importance of moving any personal information about customers from their email inboxes to your central document repository, where metadata and permissions can be applied.
- Implement strict, automated and repeatable processes as to how long you hold records and how they will be destroyed.

7

The right to be forgotten

The GDPR will allow consumers to demand that an organization deletes any data they hold on them. The original motive behind this rule was to help individuals who had been accused of some misdemeanor and had their name and details published online, but who were later acquitted. Because the original story would still be available online, anyone could find those old stories via a quick search of the person's name, and therefore get a false impression of that person's character. Being able to delete old incorrect information from the internet could be especially important in the job-seeking process.

The right to be forgotten also has other benefits for consumers too – a customer who once signed up for an account on some embarrassing website can ask for all the data pertaining to them to be deleted, or an individual may simply feel uncomfortable that a company still holds information about them. Whatever the motive, this law will allow that individual to demand that their record be removed.

Actions to take:

- As far as possible, centralize data about your individual clients in a single platform.
- Ensure that all emails and other correspondence containing personal information are moved to this central environment.
- Use a tool which can perform searches across your platforms to discover any data relating to that individual.

The last mile in GDPR compliance

This whitepaper has argued that, in many respects, success with GDPR compliance is about following sensible information management practices. The regulation should be seen as a unique opportunity to rethink your organization's approach to information governance, unify your data collection activities and also improve efficiency and customer trust.

Many leading organizations today use harmon.ie as part of their efficient information governance processes. harmon.ie is a powerful, yet easy to use tool, which makes it significantly more convenient for end users to store personally identifiable client information in the correct content repository. This boosts your organization's information governance practices – and by extension, facilitates GDPR compliance.

harmon.ie appears as a sidebar in the user's Outlook inbox which can easily be configured with the organization's SharePoint environment, as well as other platforms.

When an email of importance arrives in a user's inbox, harmon.ie allows them to simply drag and drop the email or its attachment directly to the appropriate list or library in SharePoint, where metadata (such as sender, date, creator) is automatically captured. This is much easier than the alternative – where the user must go through the tedious process of downloading the message to their computer, before uploading it again to SharePoint and manually adding metadata.



harmon.ie facilitates less onerous GDPR compliance by letting users:

- Drag and drop any emails and attachments containing PII from Outlook to SharePoint, automatically adding metadata. This means employees are much more likely to store data in a centralized place, and not keep it on their desktops, in their email inboxes or in some shadow IT environment.
- Search for content across systems. Compliance with the GDPR's 'right to be forgotten' or 'subject access requests' is easy with the harmon.ie sidebar – a user need not even leave Outlook to search across SharePoint to find sensitive data and delete it or share it with the requester.
- Prevent data leakage by encouraging best practice information governance activities, such as sharing links rather than files when sending customer information internally.

Peace of mind knowing you are GDPR compliant

harmon.ie has been designed to encourage absolute best practice for information governance among your end users. By making it as easy as possible to follow your policies in relation to the GDPR, harmon.ie can dramatically reduce your risks of GDPR non-compliance. And, with the regulation coming into effect in just a few months' time, a tool like harmon.ie also supports you to change your processes fast.

To find out how harmon.ie can play a role in your organization's GDPR compliance initiatives, contact harmon.ie today.



+1 800-624-6946



www.harmon.ie



+44 1494 358340



+49 715 26023001