The Path to Rapid GDPR Compliance

Be ready. Be certain.

Introduction

Coming into effect in May 2018, the General Data Protection Regulation (GDPR) will bring into force the biggest changes in data protection rules in two decades. It will overhaul how businesses process and handle data. It will also financially penalize organizations that are based in or operate from the European Union, or process personal data of EU residents, should they fail to adequately safeguard personal data against a breach, and report such a breach to a supervisory authority within 72 hours.

There are significant risks for businesses who are not compliant by the deadline. What is the worst-case scenario? The answer: a potentially organization-crippling fine of €20m or four percent of its annual turnover, whichever is greater. With such a dramatic risk of financial loss, it's no wonder that companies are paying serious attention to safeguarding their data.

At Code42, we are also working our way to GDPR compliance. During this transition, we have uncovered some important insights into the compliance journey, and we want to share best practice guidelines for all companies that have customers in Europe to help them prepare to meet the requirements of GDPR.

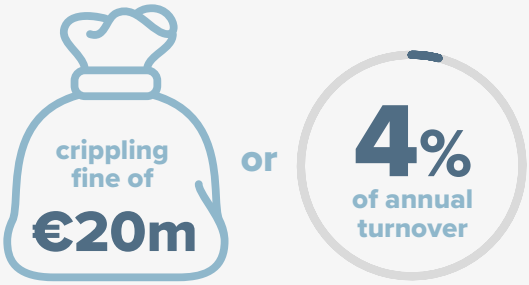
A changing landscape

At its heart, GDPR sets out rules that all organizations must follow to ensure they are protecting personal data. Overall, it is a welcome regulation for the many consumers, citizens, and businesses that believe data should be better guarded against malicious actors or accidental loss.

However, protecting data in the enterprise is not as easy as it used to be, even as recently as five or ten years ago. This is because the modern day organization is porous. People and data move freely from inside the firewall to the outside of it, and back again. In fact, Code42's CTRL-Z Study revealed that at least one in ten companies with 500 or more staff have an employee base consisting of as much as 60 percent knowledge workers. These are individuals who focus on "non-routine" problem solving that requires a combination of convergent, divergent, and creative thinking. Knowledge workers also create immense volumes of data and IP—more often than not, outside of the confines of the traditional office space. This is

The cost of GDPR non-compliance

A potentially organization-crippling fine of **€20m** or **4 percent of its annual turnover**, whichever is greater.



Code42's CTRL-Z Study revealed that **at least one in ten companies** with **500 or more staff** have an employee base consisting of as much as **60 percent knowledge workers** who often work outside of the corporate office.

evidenced by the fact that IT decision makers report that as much as half of all corporate data today is held on endpoint devices (desktop, laptop, mobile etc.) as opposed to held in a data center or within centralized servers. This makes data harder to track and protect.

GDPR compliance is therefore far from simple and straightforward. The good news is that compliance can be manageable. Here, we share the two building blocks to good GDPR compliance. First and foremost, it is about knowing what data you have, and second continuously protecting this data while also adhering to strict compliance guidelines.

Visibility mitigates risk

Visibility of your data, and knowing who/what systems handle it, becomes critical under GDPR, because this new regulation goes beyond previous notions of privacy. GDPR builds in principles of 'accountability' and a citizen's 'right to be forgotten' into EU law — changing all aspects of business and social interactions for any organization with a digital and cloud footprint. This regulation will have a high impact on all commerce organizations, especially areas like ecommerce or manufacturing supply chains, that regularly draw on and reuse multiple data sets. So knowing what you have, where it is, and how it is shared is of vital importance to maintain compliance.

In order to determine what personal data it holds, an enterprise should initiate an audit of all data sets that are held across the business. This will help to identify and understand the current business processes that create or use personal data. Keep in mind that this may include individual employee IT assets — perhaps James in sales can access personal customer data from his home office. Enterprises must know if he can, and whether his IT equipment is adequately protected.

This visibility, however, only creates a snapshot of a moment in time. What you need is technology that can forensically track data, showing where it is at any time on any device. Knowing where the data is held at any moment is critical, because visibility provides agility when there is a need to rapidly answer compliance questions. For example, with a high degree of visibility you will be able to identify data exfiltration — even before it becomes an issue. The right technology will enable alerts to be sent to relevant parties, should information be accessed or downloaded without authorization, or if there is user activity happening that is outside of established behavior patterns.

IT decision makers report that **as much as half of all corporate data today is held on endpoint devices** (desktop, laptop, etc.) as opposed to held in a data center or within centralized servers.

The **vast majority of business decision makers (95 percent)** are involved in decisions concerning the **protection of corporate data and IT security** in general.

The IT department should take the lead in purchasing and implementing this visibility solution. But it is important to remember that IT alone cannot resolve GDPR compliance in any business. Data simply touches too many areas of business today. In fact, the vast majority of business decision makers (95 percent) are involved in decisions concerning the protection of corporate data and IT security in general.

As such, once you have the right technology in place to provide you with continuous data visibility, it is time to put together a working group, or GDPR readiness program team. This group needs to consist of IT, security, lines of business managers, legal, HR, and a handful of key executives. This team has to work together to conduct a complex review of data handling, which will include a review of backup, recovery, and archiving processes across all the affected data areas. In doing so, each team member will be able to report back their gap analysis—which can then be unified into a single view of the areas to improve in order to reach full compliance.

Continuous security and compliance for all

It's been a long-held industry view that there are two types of organizations: those that have been breached, and those that are at risk of a breach. According to enterprise business decision makers surveyed within the CTRL-Z Study , more than half (51 percent) have had a security breach within the last 18 months. Of the 45 percent that haven't experienced a breach, an overwhelming majority (88 percent) believe there is a risk of one happening within view of the public in their organization in the next 12 months.

Under GDPR, organizations will be expected to report breaches within 72 hours of becoming aware of the incident. Reporting must include information on who has been affected, how widespread it is, and how/why the breach occurred. Two days is not a long time for the unprepared. Therefore, it is critical for enterprises to have their systems and processes aligned.

Code42's research shows that IT decision makers are ready for change. Seventy-one percent of IT decision makers say that there should be more investment into endpoint data protection, visibility, and recovery solutions in their organizations. In addition, 63 percent also agree that there is a real-time need to shift security strategy away from prevention and on to recovery and remediation.

More than half (51 percent) of businesses have had a security breach within the last 18 months. Of the **45 percent** that haven't experienced a breach, an **overwhelming majority (88 percent)** believe there is a risk of one happening within view of the public in their organization in the next 12 months.

51% have had a security breach

45% haven't experienced a breach

88% believe there is a risk

> Code42's research shows that IT decision makers are ready for change. **Seventy-one percent of IT decision makers** say that there should be more investment into endpoint data protection, visibility, and recovery solutions in their organizations. In addition, **63 percent also agree** that there is a real-time need to shift security strategy away from prevention and on to recovery and remediation.

Organizations need to move away from a prevention-only approach to security and focus on a balance of prevention and recovery. Recovery systems that increase visibility should be the focus of investment for the majority of enterprise organizations. Technologies that can provide centralized visibility of what data is stored across networks and devices, trace intrusions and provide an "undo button" for recovering from data loss incidents are the future. IT departments will need this level of forensic data tracking and protection to be able to take action, building it into their audit chain. After all, being able to prove what's happening, or has happened, with your data will be especially important for those that will be able to ease reporting to the likes of the Information Commissioner's Office (ICO). Moreover, being able to react quickly and with certainty to any data breach situation will become more critical, as reputational damage will also need to be considered alongside the financial risks.

This is where choosing the right data protection technology comes into play. An effective data security implementation is made up of a mix of solutions, which together provide an overarching net of protection for the enterprise. Comprehensive security stacks usually include antivirus solutions, deception technologies, encryption tools, breach detection solutions, endpoint backup, visibility, and real-time recovery systems.

Ultimately, the change will not just be around technology—although centered on it. IT, working closely with the GDPR work group, will also have to ensure that ongoing training and communication on GDPR compliance becomes part of the fabric of the enterprise. All employees need to understand their responsibility, and everyone has to work towards the ultimate goal of compliance. It will only be when all parts work in unison can the risk of a data breach be successfully reduced.

Using Code42 to increase data visibility, data protection and recovery ability

Code42's technology can track the creation of new files inside and outside the corporate network on endpoint devices such as laptops and desktops. It can also automatically help your data handlers ensure that files containing personal data are handled in accordance with company rules. Code42 offers organizations:

- The ability to increase visibility by creating a centralized view of data as it travels throughout the organization — both inside and outside of the traditional firewall. It also provides organizations the ability to forensically track the handling (which is key for GDPR reporting) of all data, and can be set up to alert the relevant data handlers that certain sets of data are being accessed by unauthorized personnel or outside parties.

- A chance to identify, in the case of lost or theft, the level of exposure and the ability to remotely lock data on an affected device to minimize risk.

- The opportunity to report at speed, and recover faster. Should your company be hit by a data breach, Code42 provides you and your employees with the ability to identify these threats and report them—as set out within the 72 hours limit of GDPR. For example, employee is attempting to exfiltrate data, an automatic alert can be set up to inform IT, who could investigate and report it. Or, if an employee was hit by ransomware, he or she could restore his/her computer to a point before the infection took place–without the need to contact IT.

Conclusion

Many organizations are already on their GDPR journey, or rapidly embarking upon it now. While change can be scary, Code42 believes it is time to start seeing the biggest regulatory change to data protection in decades as an opportunity.

It's an opportunity to change how things have always been done. A chance to build a magnifying glass into your data protection and security stack that will help your organization to spot risk sooner and report it in time. Increased visibility will not only enhance your security but also enable your company to recover faster—as problems can be identified and resolved, before they are a fully fledged threat. Fortunately, the technology that enables this agility and compliance certainty is readily available.

By implementing the right data protection and recovery technology, all companies can and will get ahead of the regulatory requirements of GDPR.

About Code42

Code42, the leader in cloud-based endpoint data security and recovery, protects more than 47,000 organizations worldwide. Code42 enables IT and security teams to centrally manage and protect critical data for some of the most recognized brands in business and education. From monitoring endpoint data movement and use, to meeting data privacy regulations, to simply and rapidly recovering from data incidents no matter the cause, Code42 is central to any organization's data security strategy. Code42 is headquartered in Minneapolis, MN and backed by Accel Partners, JMI Equity, NEA, and Split Rock Partners. For more information, visit code42.com.

Sources

[1] Code42 (2017). CTRL-Z Study, available at: https://on.code42.com/go/study-ctrlz-report/

[2] Code42 (2017). CTRL-Z Study, p. 9, available at: https://on.code42.com/go/study-ctrlz-report/

[3] Code42 (2017). CTRL-Z Study, available at: https://on.code42.com/go/study-ctrlz-report/

[4] Code42 (2017). CTRL-Z Study, p. 14, available at: https://on.code42.com/go/study-ctrlz-report/

Contact Us

code42.com
USA: 844 333 4242
UK: 0808 178 3042
Germany: +49 89 416 1169 40