Data Center | Internet of Things | Sustainability | Mobility | Security

Sustainable Technology Solutions

White Paper

Protecting Your Data Under GDPR

A guide to ensuring privacy and security throughout the technology lifecycle

Contributors

Andy Warner
Head of Corporate Services, UK and Ireland

Gary Griffiths
Global Compliance Manager

Patrick Hellman
Chief Security Officer

January 17, 2018

Introduction: Addressing New Responsibilities

With the European Union's General Data Protection Regulation (GDPR) compliance deadline of May 25, 2018, you've only got a few months to decide what, exactly, GDPR means for your company, your customers, and your employees.

New data liabilities will extend beyond simple data protection and management; it also means appropriate measures should be taken to properly sanitize business devices (laptops, mobiles, etc.) of all personal data at the devices' end of life.

Compliance with new data protection regulations is crucial to avoiding legal liability, protecting your brand, and preserving customer and employee confidence. Those who fail to meet compliance guidelines face heavy penalties. And while those penalties will be based on several factors, they fall into two key areas:

> **Failure to Comply / Technical Measures** = Up to an amount that is the GREATER of €10 million or 2% of global annual turnover (revenue) from the prior year.

> **Data Breach / Key Provisions** = Up to the GREATER of €20 million or 4% of global annual turnover from the prior year.

But being compliant by the deadline should not be your end goal; ongoing compliance should be. To make that happen, you will need to find the right partners in your journey so you're audit-ready well beyond the end of May. Responsible vendors, service providers, and IT asset disposition (ITAD) companies will be important players as you re-evaluate how you handle data and devices moving forward.

Although a June 2017 survey showed just 39 percent[1] of companies had begun working on preliminary plans to prepare for GDPR, the compliance clock ticks on. To take appropriate measures, you must first understand what GDPR is and what implications it carries for your business. This white paper will get you up to speed and offer a few suggestions for how to tackle such a large feat.

Contents

9,198,580,293 data records lost or stolen since 2013[2]

A General Overview of GDPR

When the EU published the Data Protection Directive in 1995, social media had yet to be developed. Mobile phones were just…phones. The cloud brought rain. Amazon was a Greek myth about a tribe of warrior women. As technology has changed, so has the need for better data protection.

As consumers and employees supply more and more of their personal data in the internet age—and breaches become larger and more common—it has become imperative that new protections are in place.

GDPR provides a more extensive approach to managing and using personal data, putting in place a framework of laws and regulations that create sweeping changes, many based around new protections regarding the use of data.

A Top Security Priority

A PriceWaterhouseCoopers[3] survey estimates 93 percent of U.S. companies will make GDPR a top security priority in 2018, despite an NTT Security survey[4] that shows just 25 percent of U.S. companies are aware of GDPR's effects. That same NTT survey shows that just half of European companies are aware of GDPR's effect on them, with the U.K. registering the lowest awareness. These issues aside, companies are expecting to spend anywhere between a million and 10 million dollars to meet compliance regulations.

Global Application

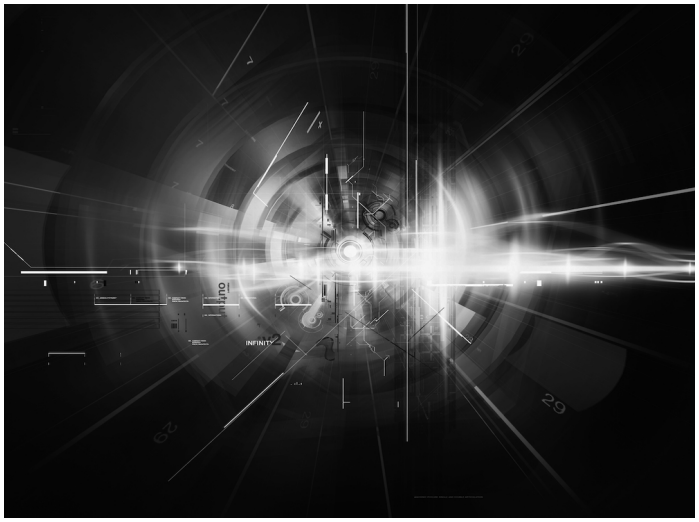
GDPR doesn't just affect European companies, either. Any business collecting and handling the personal data of EU citizens must comply even if they're based outside the EU. This includes employees of a company and their clients, customers, etc. As such, these changes bring new liabilities for the vast majorities of businesses around the world.

GDPR Compliance Criteria

While much has been left to interpretation in prior regulations, GDPR strips away any ambiguity around who must fall in line. If you meet any of the following criteria, GDPR affects you.

- You have a business presence in an EU country.
- You have a business presence outside an EU country, but you collect and process the personal data of EU citizens.
- Your company consists of more than 250 employees.
- Your company has fewer than 250 employees, but you process sensitive personal data.

Knowing the severity of fines and sweeping changes that are coming, it's critical—if you meet any of the criteria above—that you begin working towards compliance today. Your IT team will be an ally, according to a recent survey by Blancco. Blancco found that IT professionals inside and outside of Europe (65 percent) are keen to implement data protection practices similar to the GDPR framework[5].



Changes in Liability

Under previous data protection legislation, the liability for a data breach lay with the entity that created the data. When a breach occurred, that party was fined. For example, when an IT asset disposition (ITAD) company failed to properly remove data from health trust hard drives before selling those hard drives to another company, the trust was fined, not the processing company.

Now, however, GDPR creates shared liability between the data controller (the company that creates the data) and the data processor (all other parties involved). As such, both parties could be fined for not properly handling personal data.

> **Data Controller—**The natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means of the processing of personal data*

> **Data Processor—**The natural or legal person, public authority, agency or other body which *processes personal data on behalf of the controller*

Beyond the enormity of potential fines for both controllers and processors now, you will want to turn a discerning eye to current contracts with companies who process customer or employee data to ensure GDPR compliance. This includes supply chain vendors, solution providers, subcontractors, ITAD partners, and channel partners.

And based on the fact that many of these companies may not be financially prepared in the event of large fines nor have the resources to partner on GDPR compliance in the first place, it becomes more important to work with financially stable and reputable companies.

Summarizing the Articles

GDPR protects a wide variety of personal data, including basic information, such as names and addresses; web data, including IP addresses, cookies, and RFID tags; health and genetic data; biometric data; racial or ethnic data; political opinions; and sexual orientation.

For a deeper understanding of how GDPR affects the data your enterprise processes, it's critical to know about specific changes GDPR brings.

Breach Notification

Data breach notifications are now mandatory and must be made public within 72 hours of said breach. Under GDPR, data processors must also notify customers and controllers "without undue delay."

Right to Access

To shift transparency, customers now must actively provide consent and receive notice from the controller about how their personal data will be used. The controller must provide a copy of the information—free of charge—that informs the subject of what data is being used, where it's being used, and for what purpose.

Right to be Forgotten

Customers have a right to request the data controller erases his/her personal data and stop sharing said data. However, there are conditions for erasure requests further defined in article 17, such as data is no longer relevant or the subject has withdrawn consent.

Data Portability

Essentially, customers have the right to request their personal data from a controller so they can share it with another data controller.

Privacy by Design

The privacy by design concept calls for companies to build data protection into the design of data collection and processing systems rather than as an add-on later. This means the data controller is now responsible for implementing technical and organizational measures that meet GDPR requirements. Many believe privacy by design is the biggest challenge facing enterprises[6].

Data Protection Officers

This article outlines internal record keeping requirements. The appointment of a Data Protection Officer (DPO) may be mandatory for controllers or processors who regularly and systematically monitor "data subjects on a large scale," or collect special categories of personal data (race, ethnicity, political opinions, religious beliefs). This also applies to data "relating to criminal convictions and offences."

Increased Territorial Scope (Extraterritorial Applicability)

Perhaps the largest change companies face is the jurisdiction specificity. Previous language around territorial scope was unclear and was interpreted in myriad ways. GDPR rectifies that by defining, in strict terms, that the processing of EU citizens' data anywhere in the world is subject to GDPR.

Consent

This article makes it clear that companies should avoid legalese in any request for consent language. All forms must be easily accessible and plain language consent must be distinguishable. Parental consent for data on children under 16 or 13 is also required, depending on the EU country of which they are a citizen.

Penalties

As mentioned previously, penalties fall into two categories: technical and key provisions. The maximum fine organizations in breach of privacy by design concepts face is up to 4% of annual global turnover or €20 million (whichever is greater). There is a separate, tiered approach for less significant violations.

Compliance Concerns for Non-EU Companies

Certain industries—healthcare and finance, for example—have experienced a patchwork of laws and consumer protections under current, somewhat ambiguous European regulations. This patchwork runs the gamut from how telemarketers access personal information to measures designed to prohibit deceptive marketing and advertising practices. European-based organizations have, for years, been confused and uncertain as regulatory bodies—and the organizations themselves—make independent interpretations of this patchwork. Uniting these interpretations within the new GDPR framework is going to take time, money, and resources, in numbers some organizations still fail to recognize.

Organizations with operations in the EU must gain control of data quality in the months leading up to the GDPR deadline. This includes discovering and classifying data, mapping data flows, and analyzing data gaps before considering other critical factors like security and audit protocols. According to Patrick Hellman, chief security officer of Arrow Electronics, organizations "need to start thinking about why [data is] collected, how it's protected, and how it is destroyed when it has reach the end of its useful life."

According to Forrester, the International Association of Privacy Professionals (IAPP) expects that firms will need 28,000 new Data Protection Officers (DPOs) in Europe alone[7].

Raising the Bar on Privacy Protections

Love it or hate it, GDPR is a long-overdue step in helping companies raise the bar on consumer privacy protections. With only a few months until the compliance deadline, it's critical to begin preparing systems, processes, and staff for coming changes. This means making all stakeholders aware of how new rules affect them and how data must be handled to stay compliant.

> "Half of organizations across the EU and the U.S. are unaware of the new European General Data Protection Regulation (GDPR). Even more worrisome, the rate of awareness is lowest among tech companies[8]."

There are specific contractual and legal steps you must follow to meet compliance guidelines. Knowing it takes quite awhile to make changes in legal processes, here are six steps you should be implementing in your organization, right now.

1. Discovery/awareness: What do you have, where did it come from, and with whom is it shared?

2. Create a data protection plan: Many already have one in place, but you'll need to review and update yours.

3. Assign/hire a Data Protection Officer (if you need one): GDPR does not say this must be an explicit position, but you'll want to avoid conflicts of interest. May be virtual or full-time.

4. Create an accountability framework: This may be a requirement for you under GDPR. If this applies to you, you must be able to prove policies and procedures comply with defined protection principles. You must also provide DPO contact info.

5. Review and update all policies: This includes retention policies, privacy policies, and personal data notifications. These should be stated in plain language.

6. Perform due diligence of third-party vendors: Make sure they understand GDPR compliance, are abiding by it, and are not violating cross-border data transfer rules.

Getting Serious and Taking Action

New requirements under GDPR are anything but trivial. If you haven't started addressing the changes required of your organization already, you will be forced to play catch-up. Or worse, you'll be paying heavy fines.

> "GDPR is about ongoing compliance. Firms that approach this task as a one-off effort will face the risk of failure. Therefore, privacy and security pros must make sure to continuously monitor, adjust, and document their compliance strategies[9]."

Having the right partners, those with the breadth of knowledge, size, and experience, and who understand the importance of your customer and employee data, will be key in meeting and maintaining compliance.

While initial discussions will naturally be around cloud capabilities and two-factor authentication, you'll also need to consider what to do with devices when they reach end of life. No one is talking about proper disposal of laptops, mobiles, hardware, and other enterprise equipment...yet. But they will be, probably as an afterthought. Be sure you're considering the entire data lifecycle as you put together a compliance plan, review vendors, and make changes.

Yes, there is a lot of work to be done. But with the right help, you can meet compliance requirements on time and take advantage of new opportunities to get ahead.

About Arrow

Arrow Electronics (www.arrow.com) is a global provider of products, services and solutions to industrial and commercial users of electronic components and enterprise computing solutions. Arrow serves as a supply channel partner for more than 125,000 original equipment manufacturers, contract manufacturers and commercial customers through a global network of more than 465 locations serving over 90 countries.

Arrow's Sustainable Technology Solutions business (www.arrow.com/s-tech) is a worldwide provider of full technology lifecycle services and solutions designed to deliver data security, environmental responsibility, process efficiency and economic value. With specialized expertise in reverse logistics, IT asset management, and supply chain optimization, Arrow enables organizations to uncover hidden value in their technology supply chain and increase sustainability at the end of the technology product lifecycle.

References:

1. https://info.trustarc.com/Web-Resource-PrivacyGDPR-Research-Q22017_TY.html?asset=JT190EEP-669&alild=41289145
2. http://breachlevelindex.com/
3. https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf
4. https://www.nttsecurity.com/docs/librariesprovider3/resources/global_report_risk-value_2017_a4_uea_v6.pdf?sfvrsn=a06281fa_2
5. https://www.blancco.com/resources/rs-eu-gdpr-a-corporate-dilemma/
6. Brief: You Need An Action Plan For The GDPR, Forrester, Oct. 14, 2016
7. The Five Milestones To GDPR Success, Forrester, April 25, 2017
8. The Five Milestones To GDPR Success, Forrester, April 25, 2017
9. The Five Milestones To GDPR Success, Forrester, April 25, 2017

Five Years Out

Arrow Electronics, Inc.
Sustainable Technology Solutions

9201 East Dry Creek Road
Centennial, CO 80112, USA