# All You Need To Know About GDPR

## An Argent Guide

# Introduction

According to a leading provider of research and analysis on security and risk management, in just the last ten years 15 major global data breaches have been reported impacting billions of user accounts including:

| | |
|---|---|
| **2006** | |
| TJX Companies | 94 Million Accounts |
| **2008** | |
| Hartland Payment Systems | 134 Million Accounts |
| **2011** | |
| Sony PlayStation Network | 77 Million Accounts |
| RSA Security | 40 Million Accounts |
| **2013** | |
| Target Stores | 110 Million Accounts |
| Adobe | 33 Million Accounts |
| **2014** | |
| Yahoo | 1,500 Million Accounts |
| eBay | 145 Million Accounts |
| JP Morgan Chase | 76 Million Accounts |
| Home Depot | 56 Million Accounts |
| Office Personnel Mgmt | 22 Million Accounts |
| **2015** | |
| Anthem | 79 Million Accounts |
| **2016** | |
| Adult Friend Finder | 412 Million Accounts |

Not only did consumer confidence in these companies plummet, so did the companies' market valuation. For instance, the Yahoo breach caused a USD 350 million reduction in its sales price to Verizon. And then there are the dozens of lawsuits, many claiming negligence.

To combat breaches such as these and the ever-growing threat of ransomware, governments around the world are frantically establishing guidelines to guard sensitive electronic data.

The most stringent by far and the one with the largest penalties is GDPR.

*"Oh, that does not affect us in America – that's just for the people across the pond…"*

Wrong. Dead wrong. Potentially very, very expensively wrong.

# What Is The EU GDPR?

Every day it seems another government agency somewhere in the world creates another standard for IT compliance. CJIS, SOX, PCI, HIPAA, GLBA, FISMA, and APA are among the ever-growing list of requirements being imposed on businesses and local, state, and federal agencies. As soon as your exhausted staff completes all the requirements of one external auditor, another arrives at your door with a completely different set of requirements. This is a dizzying cycle that is causing even the largest of IT departments to feel overworked and overwhelmed. And with tightening budgets, CIOs are being forced to do much more with much less.

The solution to this frenzy is to get ahead of the curve – to begin preparation for compliance laws as soon as they are announced. The latest edition to the compliance standards is the "**European Union General Data Protection Regulation.**" As the name suggests, EU GDPR set of regulations was approved by the European Union on 14 April 2016 after four long, tortuous and painful years of internal debate and deliberation

**The most critical part of this massive law is that it affects any company or government agency anywhere is the world that does business with one or more EU residents, regardless of a company's location.**

This law repeals and replaces the established compliance rule known as Directive 95/46/EC, known widely as the "Data Protection Directive" (DPD), which was designed to protect personal data. GDPR, with its 99 articles and 173 recitals, goes into effect on 25 May 2018. With time counting down, it is imperative that organizations begin preparing for GDPR immediately.

# Will GDPR Impact Me Directly?

Ontologically, GDPR is not much different than its DPD predecessor. The core values are the same, but individuals' rights have been expanded dramatically. Perhaps the most welcome aspect of GDPR regards the sale of individual private data. It is likely that right now your junk folder is the largest folder in your mailbox. The reason? Companies do not have to ask your permission to opt-in to mass emails and spam. Many online marketers have purchased your personal data from shared databases without your consent.

With GDPR, this will be a thing of the past. Just think about it – no more fake emails from "Bob" at Amazon.com.xyz or unwanted spam regarding the next great solution to male pattern baldness. Further, it will be illegal to combine data from multiple sources to build a profile of you, thus protecting your public electronic dossier. You will be granted the "right to be forgotten" in which you can require a company to completely erase all of your personal records from their systems. You will also have the right to transfer your personal data from one "data controller" organization to another at your discretion.

Consent to collect and use your data must be "a freely given, specific, informed and unambiguous indication of the individual's wishes." In addition, data related to children under 16 years old must be authorized by a legal parent or guardian to engage in most online data collection services.

# How Will GDPR Impact My Company or Department?

As the saying goes, "with great power, comes great responsibility." Reality is that protecting customer data isn't a free endeavor. To be sure, it will take a lot of human resources, operational costs, and managerial effort to ensure GDPR compliance. **However, failure to do so will incur a fine on your company for up to 4% of your previous fiscal year's global revenue.** Organizations with foresight agree the hefty fine and net losses from ensuing customer evacuations more than make up for the labor required to become GDPR compliant.

# How Can My Company Prepare for GDPR Compliance?

GDPR strongly recommends the adoption of certification schemes to help ensure compliance. The International Information Standard (ISO 27001) is the only internationally recognized security standard that currently conforms to the GDPR guidelines.

ISO 27001 recommends that each corporation appoint a Data Protection Officer (DPO) who is trained and certified with ISO standards. Under the Network and Information Security Directive, companies will also be required to report all data breaches within 72 hours of the occurrence and notify affected consumers "without undue delay." Additionally, businesses should immediately begin to identify: what personal data is held on the network, which users have permissions to access the data, what processes are in place for securing that data, what data is transferred outside of the company, and how the data is expunged once it is obsolete.

# What ISO 27001 Guidelines Must IT Be Concerned About?

This checklist outlines the ISO 27001 guidelines for compliance and should satisfy the portion of GDPR requirements for IT mandated for auditing.

Today, now, as you are reading, Argent Software fully meets each of the following criteria

- A.9.4 Monitor all security accounts with elevated privileges
- A.9.5 Monitor access to all proprietary source code materials
- A.12.1.3 Implement a capacity management process
- A.12.2.1 Verify active operation of malware
- A.12.3.1 Verify backup operations in accordance with policy
- A.12.4.1 All appropriate event logs must be maintained
- A.12.4.2 Data Archiving must be secured
- A.12.4.3 All Sysadmin and Sysop logs must be maintained
- A.12.4.4 All time clocks must be synchronized
- A.12.5 Monitor installation of software on operational systems
- A.12.7.1 Provide systems audit with minimized business interruption
- A.13.1.2 Monitor security related SLAs
- A.14.3.1 Monitor access to test data
- A.16.1.2 Immediately report on information security events
- A.17.2.1 Monitor failover systems and disaster recovery facilities
- A.18.1.2 Monitor the use of unlicensed software

# How Can Argent Get Your Company GDPR Compliant In One Afternoon?

As we say at Argent, "you cannot improve upon that which you don't monitor." How can you know if you are improving a system or group of systems if you are not monitoring them for a baseline?

We use this same principle of monitoring to our approach in governance. With staff certified in regulatory guidelines, Argent has quickly become a household name for electronic data monitoring and audit report automation.

GDPR is likely to affect most departments within your organization including: Legal, Human Resources, Insurance, Security, Procurement, Marketing, and Public Relations. There is much work to be done for each of these departments' policies and procedures, but for Information Technology departments, Argent does all the heavy lifting for you.

The Argent solution easily and quickly ensures your IT department is GDPR compliant. Our comprehensive approach consists of the following six methods for personal data protection that should not only satisfy your auditors, but your boss too and the CFO as well.

**Method 1: Proactive Monitoring and Alerting for Data Breaches**

Argent for Compliance offers 18 different types of customizable alerts for all critical network system events. In the unfortunate event of a data breach, Argent will immediately notify your team so you can take immediate action. Not only is real-time monitoring and alerting critical for you to deploy countermeasures, but the sooner you learn of a breach the faster you can report it and avoid costly fines. Argent for Compliance can monitor all Windows Server events, all Linux/Unix message logs, all network device SYSLOG (such as firewalls, routers, switches, etc.), all enterprise application log (such as IIS or SQL), and all iSeries logs.

**Method 2: Proactive Monitoring and Alerting of Network Shares**

Under GDPR your company will be required to list all shared locations on your network that store personal private data. As an example, you might have an intranet page that lists client contact information. Argent can watch all access to the source files, keep a record of changes made to the files or folders, and alert you if unauthorized users attempt to modify the data. Argent can even display the IP address and username of the person who accessed the data.

**Method 3: Data Archiving – Making The External Auditors Believe**

All data relating to compliance must be retained for auditing with the capability of rapid analysis. Argent stores all of its compliance data into one centralized SQL Server (or other ODBC database). The benefits of using SQL Server are that access to data can easily be controlled and quickly accessible to authorized personnel. Argent also intelligently stores the data to prevent data bloat. As Argent analyzes the myriad data points from a plethora of sources, only pertinent data is collected and stored. This data mining approach prevents the unnecessary writing of records in the SQL tables, which over time can cause database corruption. Extraneous data can also affect database backups and general SQL performance. Our database has been carefully organized for maximum efficiency with minimal overhead. Argent also gives you total control of data retention, allowing you to specify how much data you collect and how long you keep that data.

**Method 4: Bulletproof Design**

**On 25 May 2018, when GDPR goes into effect, auditors will not accept any excuses for missing data collection or lack of preparation.** Thus, the Argent solution has been designed to be completely robust and scalable and without a required agent. When it comes to GDPR compliance, you need proven solutions you can rely on and only with Argent can you be fully confident that your compliance data is secure. Argent has built-in fault tolerance, which can handle slow or erratic networks and hardware failures. In large environments, Argent can be deployed in a distributed fashion allowing for load-balancing to collect over 1 TB of data daily and our optional regional data collectors (Trusted Agents) are provided at no additional cost. With Argent for Compliance you can set it and forget it.

**Method 5: Scheduling Automation**

Without getting too technical, Argent has three independent scheduling engines.

The first was built with resource optimization in mind. It allows the multi-threaded Argent system to efficiently utilize its host's resources to provide real-time collection, scanning, and consolidation of data. However, the system can also be scaled down for periodic data gathering after hours, on the weekends or during holidays. You can even pause data collection during maintenance windows or especially busy times such as during nightly backups.

The second schedule engine has customizable calendars for alerting purposes. You can specify the types of events you want to be notified of and who gets those notifications. For instance, your security team may receive email notices of hacker attack attempts from your firewalls during regular business hours, but in the evening the messages could be sent via SMS text to an on-call operator. Alerts can also be automatically escalated to a supervisor or manager if no one has responded to the event in a timely fashion.

The third schedule engine automatically distributes hourly, daily, weekly, monthly, or quarterly reports. You decide who gets what data and how frequently the reports are generated. There will no longer be any guessing of what data you or the GDPR auditors can access.

**Method 6: Targeted Reporting**

Argent's reports are not only well-organized and customizable, but stunning too, making them easier to read and understand. Argent comes with 32 GDPR reports out of the box. As an option you can also design and build your own GDPR web-based reports complete with your company logo.

You can then schedule the reports to be sent via email or saved to a network location. Argent uses Active Directory accounts to prevent reports from being generated or seen by wandering eyes. A typical table-based GDPR report lists: the date of an event, the event details, the authenticating Domain Controller, the IP address of the computer (or network device) responsible for the event, the username (if applicable) associated with the event, and pertinent event details. This simple format makes it easy to distinguish brute force attacks from

legitimate failed logon attempts, for example. Argent Reports completes Argent's 6-method comprehensive solution for GDPR compliance monitoring.

Can your organization afford the fines resulting from being unprepared for the new EU GDPR law?

**Friday, 25 May 2018 is closer than you think – are you ready or will you be one of the sad unfortunates shelling out 4% of your previous fiscal year's global revenue?**

**It is urgent for you to contact your Argent account representative today to schedule a demo of Argent for Compliance so your IT team can avoid the stress of the last minute, inevitable mandate from your CEO in May, 2018.**