
ardoq
NEW EA
MAGAZINE
Ardoq's magazine to help avant-garde CxOs and progressive enterprise architects understand how their people, processes, and data interconnect to provide valuable insights.
GDPR EDITION

NEW EA

CONTENTS

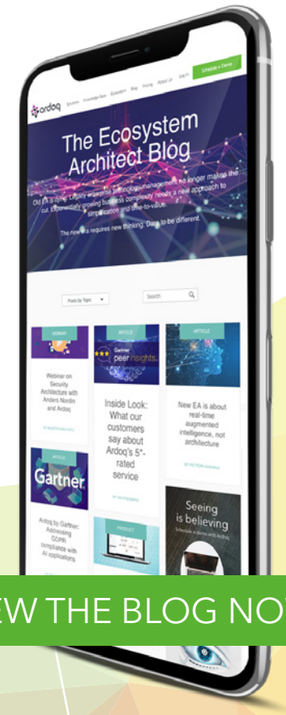
FOREWORD **NEW EA**

The Ardoq blog is the place to go for all the latest news, views, insights, and updates on everything to do with EA. But if you don't have the time to drop in and have a look around, don't worry – we're bringing our most popular blog posts to you in our magazine, New EA.

In this issue we look at the ongoing challenges posed by GDPR, highlighting how costs can spiral out of control without careful management and planning. We also explore the importance of AI and automation when it comes to GDPR compliance, and why organizations should look at the opportunities created by GDPR as well as the risks.

Happy reading!

Petteri Vainikka,
CMO, Ardoq



VIEW THE BLOG NOW

ARE YOU WILLING TO WASTE $1 MILLION ANNUALLY ON GDPR COMPLIANCE?

As everyone has realised, May 25 2018 was not the beginning and the end of GDPR – it was just the kick-off. For GDPR compliance with associated investment in people and tooling, this means that whatever your organization invested in becoming GDPR compliant before this date has most likely transformed into an ongoing compliance cost.

In fact, in December 2017, Forrester predicted that maintenance budgets for GDPR and ePrivacy compliance are larger than initial budgets – and anticipates they'll only get larger. Forrester further added that 58% of enterprises expect an annual maintenance budget of over $1 million, and a whopping 88% anticipate an annual maintenance budget above $500,000. Clearly, regulatory compliance with the GDPR has a material GRC budget impact, and cannot be sidelined as a mere one-off legal and/or consultancy expense.

> **"May 25 2018 was not the beginning and the end of GDPR – it was just the kick-off"**

Of course, the vast majority of GDPR compliance cost is due to associated people cost. This is both direct (dedicated DPO or equivalent) and indirect (repetitive disturbances from cumbersome GDPR data mapping and documentation needs on business process, data, and application owners and users), and is in many cases exacerbated by a lack of suitable tooling. The result is unnecessary complexity, confusion, and workload for everyone.

The GDPR Article 30 requires that a Data Controller "shall maintain a record of processing activities under its responsibility". Article 30 compliance can of course be demonstrated quite simply by small organizations with few processing activities and limited data traffic, but most medium and large organizations face a very different scenario.

For organizations providing a diverse range of services and products to hundreds of thousands of customers, with technologies that vary from service to service, country to country, and office to office, 'simple' is a rarely-used term.

How can larger organizations operationalize GDPR compliance cost-efficiently and with minimal disturbance to business operations, and to those responsible for product and service P&L?

In February 2018, market analyst Gartner predicted that by 2021, more than 60% of large organizations will have a privacy management program fully integrated into the business, and that already by 2019, half of the world's large companies that process personal data will perform privacy impact assessments. However, despite this, only 10% will have a defined, automated PIA process in place.

OPERATIONALIZING GDPR COMPLIANCE

> Initial data flow mapping work identified 200+ processes in scope for GDPR compliance, **and the detail of each needs to be documented and kept up-to-date continuously."**
>
> - Ardoq customer

ARE YOU APPROACHING GDPR COMPLIANCE CORRECTLY?

In our research, several things stand out as critical success factors. Clearly, automation, two-way reusability of data mapping and documentation, ease of gap discovery, and no-UI data input ability are key to cost-efficient GDPR compliance. Attempts to manually solve (via Excel, for example) the GDPR's challenges simply fall short, as do attempts with unsuitable tools. We've compiled a list of things to look out for to help you get started, and to assess your current GDPR compliance approach.

Watch out for these warning signs:

1. Data flow mapping methods and hosting solutions are not capable of accurate and timely reporting of data flows.
2. Methods prescribed by external consultants do not support actual business process improvement or data minimization
3. Solution does not support out-of-the-box visualization of data flows that are understandable to business process owners
4. Visualizations of data flows show only basic metadata, with no ability to drill down into the maps
5. Metadata which would allow for effective risk management is not supported
6. Solution does not support out-of-the-box collaboration and stakeholder involvement, including no-UI data input ability
7. Audit logs, user rights management, and change management are limited or lacking entirely

Look for these positive indicators:

1. Easy to engage multiple business process owners and other data handling stakeholders without need for new software training
2. Wide range of out-of-the-box data flow, process flow, criticality landscape, and other visualizations
3. All visualizations are auto-generated and offer the ability to drill into the maps
4. Supports automated gap analysis, customizable by business process criticality as well as data classification severity
5. Enterprise grade user authentication security options, audit and tracking capabilities
6. Ready yet customizable templates for GDPR data mapping and DPIA assessment and automation
7. Supports and integrates with other security, quality, process, and IT management solutions already in use
8. Has full RESTful API

> "By 2021, more than 60% of large organizations will have a privacy management program **fully integratied into the business.**"
>
> - Gartner, February 2018

ARDOQ BY GARTNER ADDRESSING GDPR COMPLIANCE WITH AI APPLICATIONS

Ardoq is proud to have been selected by Gartner as a leading AI-driven application to address GDPR compliance. For more details, please see 'Gartner Market Insight: Address GDPR Compliance With AI Applications'

The EU General Data Protection Regulation (GDPR) took effect on 25 May 2018, yet according to Gartner, 'by year-end 2018, fewer than 50% of companies affected will be compliance-ready'. To remedy this, Gartner suggests that technology business unit leaders responsible for compliance platforms should consider AI applications to ease process complexities.

GAINING A COMPETITIVE ADVANTAGE

While compliance dashboards are nothing new to compliance-and-risk based activities and tools, AI applications go one step further, offering targeted summary reports for business risk managers, data protection officers (DPOs), and key executives, all made available to non-technology-savvy business stakeholders. Such personalized reports are delivered based on event triggers in the ecosystem, and pushed to audiences where they are.

AI applications offer valuable information augmentation to contextualize key data. They go from what, to why, offering instant remedial action suggestions. Finally, machine learning underpinned by graph queryable searches automatically assesses enterprise intelligence graphs for gaps and changes across layers covering complex IT landscapes, business process models, and ecosystems. Scalable property graphs allow for information management and analysis far beyond human visual analysis or conventional database models.

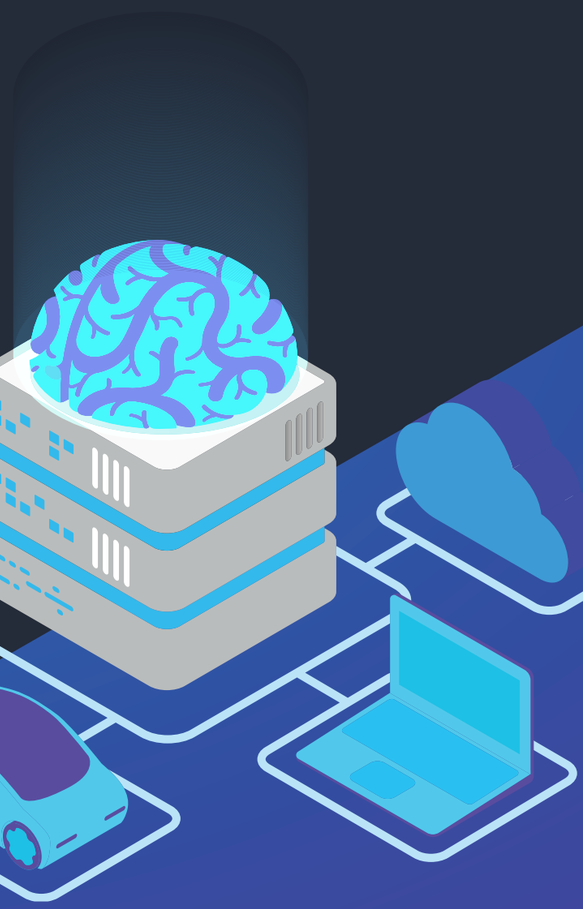
ardoq

EXPERIENCE FULL-SCALE USE OF AI TO ADDRESS GDPR COMPLIANCE IN ARDOQ

- Auto-generate GDPR crowdsourcing surveys from any data model
- Auto-complete fields in-tool and in-survey for high-fidelity structured data collection
- Auto-update visual dive-in presentations, regardless of where deployed
- Perform continuous gap discovery with smart notifications (also to third party apps e.g. Slack)
- Find duplicated/synonymous data in the data graph for higher data coherence and quality
- Automatically adjust graph analytics insight perspective to user's preferences

THINGS TO LOOK OUT FOR FROM ARDOQ IN AI

- Ability to answer to complex business questions across multiple privacy and other architecture domains using natural language (Chatbot user interface that combines NLP with powerful graph search capabilities)



CREATING STRUCTURED **GDPR COMPLIANCE DOCUMENTATION**

We've met with any number of companies, large and small, working towards GDPR compliance. We didn't start out as GDPR experts, but we've learned a lot from our customers about the common challenges that companies face now, are likely to face going forward, and the mistakes that can be made when getting started with a complex compliance project.

At a high level, we've learned three key lessons:

1. Compliance is a continuous process, not a periodic one
2. It's important to involve domain experts in your organization to help get an accurate understanding of the current status of systems and processes
3. If you think structured with your compliance documentation, not only will it make the compliance process easier, it will also empower you to use the data you collect for other digital transformation initiatives

This post will explore why creating structured compliance documentation is the best approach for your business.

BE STRUCTURED

GDPR compliance impacts every part of an organization. Not only that, it's a continuous process, and will likely alter the organization's culture and how it operates. When going through such a process, it's essential to be able to accurately document what you've done.

Documenting your GDPR compliance in a structured way will make it easier to discover and prioritize compliance gaps, and lay the foundation for value-adding projects beyond GDPR.

STRUCTURED VS. UNSTRUCTURED DATA

The first step of creating structured documentation is to identify the important attributes of an object. For example, when documenting an application, you'll want to know if it processes personal data. When documenting personal data, you'll want to know if consent was gathered.

These attributes should have defined input types, and include any relevant restrictions. Knowing what values an attribute may have makes analysis easier, and will ultimately give you greater confidence in the accuracy of the documentation.

One example of unstructured data would be a Word document; even if all the important information is present, it would be difficult to, for example, compare the number of data subjects in one document to another, or to sort the data. Even when using a structured tool like Excel, it's possible to enter data in an unstructured way.

DESIGN DOCUMENTATION FOR REUSABILITY

In the process of documenting your GDPR compliance, you'll be collecting information about the core of your organization, and subsequently finding out what makes it tick, and what makes it competitive. Personal data drives most organizations, whether B2C or B2B, while things like HR data and customer/vendor data are key to competitive success.

If you're investing the time to document these things for GDPR compliance, why not design the documentation in such a way that it's reusable for future projects?

In addition to making data analysis more straightforward, structured documentation makes it much easier to import your data into other tools in the future, reducing the amount of time needed to get started with new projects. Unstructured data, on the other hand, offers very little reusability.

VALUE BEYOND GDPR COMPLIANCE

GDPR requires an understanding of core business processes, applications, and infrastructure. The high-risk nature of GDPR means that most organizations have made compliance a top priority. Leveraging GDPR focus to create structured, up-to-date documentation can lay the foundations for:

- Performing risk analysis
- Identifying the biggest challenges in a digitalization process
- Changing IT vendors

These are all small wins, but they add up to reduce the total cost of ownership of your compliance documentation. Take steps now to design a structured GDPR compliance documentation strategy, and your business will reap the benefits.

ardoq

WHERE ARDOQ FITS IN

In order to realize the benefits of GDPR compliance, you first need to get a clear understanding of what personal data exists in your organization, where it's used and stored, who has access, and the reason for having it.

Ardoq allows you to create structured documentation of all of this data, then use it to generate up-to-date visualizations, and run automated gap analysis to spot potential issues early on.

BETTER, FASTER SECURITY ARCHITECTURE **WITH MEASURABLE ROI**

FIGHTING CRIME FROM AN ICT DEPARTMENT PERSPECTIVE

A police force's ICT department plays a key enabling role in supporting police activities, helping the police solve and prevent crime (including cyber crime) by developing, operating, and managing more than a hundred IT systems.

Now, the ICT department is on an exciting journey. They're revolutionizing how data protection, risk assessment, and security are handled – assisted by their data-driven graph Enterprise Architecture platform.

In the digital era, speed, agility, and central visibility into all systems, documents, and regulations – such as GDPR – become critical to operations. With the help of Ardoq, a data-driven enterprise graph platform selected by a growing number of innovative global organizations for their compliance, governance, and digital transformation, a police force's ICT department identifies and addresses threats, vulnerabilities, and potential risks – and, most importantly, is able to identify cost-efficient mitigations.

But it hasn't always been this way.

WORKING WITH AN IMPERFECT SYSTEM AND SCATTERED INFORMATION

With many EA solutions, documents and system overviews are not centralized properly, and the focus is on architecture modeling, not true analytics. This affects the response time, and makes risk assessment analysis dependent on manually connected information sourced from multiple different systems.

"It was exceedingly difficult to show the connections and dependencies between software solutions, threats, and risks; and to justify interpretations with strong enough insights to make informed decisions based on hard data."

- Enterprise Architect, police force

This was the 'data crime' the police force were themselves committing. Previously, the ICT department would store, aggregate, and analyze data in different places. For example:

- Data Classification was done in Excel spreadsheets
- The System Overview was performed using tools such as Visio or Gliffy
- Excel was often the preferred option for Threat Modelling
- Word documents and Excel spreadsheets were primarily used to evaluate and analyze Risk Management

There were numerous other limitations to the old system, such as:

- Not allowing peer collaboration
- Information was often dependent on its owner
- A lack of instant, up-to-date, or peer-validated information
- Visualizing future scenarios and their impact was often taken at face value, without digging deeper into the rationale behind business decisions. At the same time, communicating complex analysis to business executives in a coherent and consistent way was a very difficult process
- Decisions related to risk management were often taken by analyzing the data from different and isolated sources, and, even if the results were correct and the threats and vulnerabilities were detected/highlighted, the insights were often difficult to demonstrate with sufficient hard evidence.

You can easily see how poorly such an approach scales with increased complexity and more demanding data and privacy laws,"

says the Enterprise Architect.

A MOVE TO AN AI-ENHANCED EA TOOL

To mitigate such challenges, in 2017 the police force's ICT department moved their Security and Enterprise Architecture to a new era of EA with Ardoq; one that is data-driven, highly-automated, and offers interconnected perspectives and real-time insights using advanced graph analytics.

Moving from IT architectures to business architectures represents an incremental shift in the role and value of enterprise architecture. Moving to Enterprise and Ecosystem Intelligence on-demand is a radical one."

- Enterprise Architect

Ardoq's data-driven graph EA platform allows the police to obtain relevant, real-time insights across all processes and systems. It enables collaboration across teams, and democratizes data collection and analytics output access based on agreed user rights levels.

The ICT Services wants to become faster, better, and more efficient when it comes to detecting and addressing risks, threats and vulnerabilities. We need a complex yet user-friendly EA solution that focuses on augmented analytics and visualization for decision support, in order to ensure against IT and privacy breach incidents."

- Enterprise Architect

COLLABORATION, DEMOCRATIZATION, AND CONTROL

Being able to make well-informed decisions is one of the most significant outcomes of using Ardoq for the police force's ICT department.

They now have a clear overview of all systems, applications, users, and data, as well as all possible relations between and across them. It creates a structure for digital age security governance, and different departments can collaborate to build up the documentation.

System owners, infrastructure teams, and developers can use Ardoq Surveys to document information. Their contribution is monitored, and the results create automatic updates into the Enterprise Intelligence Graph that Ardoq provides. The Security Architect can now have a better overview and, at the same time, identify immediately different breaches into the system, or threats and vulnerabilities. This can now be easily communicated to the management using heat maps, one of Ardoq's many out-of-the-box visualizations for complex data relationships.

You have the complete overview and you can dive into the specifics. That will bring you enormous credit and will support your suggestions in front of decision-makers, as one can dig into a level of discussion they have never seen before. When it comes to risk assessments and decisions, you can show the whole picture, sum up the info into a heat map, or dive into a specific vulnerability and debate it. Only like this one can understand the development of risk and create a risk treatment plan."

- Security Architect, police force's ICT department

ANOTHER CASE SOLVED

With state-of-the-art tooling usage being scaled across the organization, the next phase for the ICT department is to re-educate people away from their reliance on standard office tools to document risk and security related information. By doing so, it will enable enterprise-wide risk and security information to be fully connected and analytically accessible. Just as risk assessment itself is a continuous process, so is the police's adoption and usage of Ardoq's leading EA solution.

GDPR TEMPLATES FOR **GAP ANALYSIS**

Recently, we've been working closely with our partner, Capgemini, to help a shared client in its journey towards GDPR compliance. This process provided valuable insights into how similar projects have traditionally used fragmented tools – Excel, PowerPoint, and Visio, for example – to gain an overview of expansive and complex projects. And, while these tools all have their own strengths and purposes, when used in this type of scenario, teams are setting themselves up for failure.

GDPR COMPLIANCE GAP ANALYSIS

To begin, the client looked at all domains, processes, and supporting application services across its international organization. There was a need to identify:

1. What type of data was being handled
2. What legal basis supported that handling
3. The specific purpose it served

Then, the level of compliance with each of the GDPR principles was assessed. Compliance gaps, as well as areas requiring additional investigation, were subsequently noted and documented.

And, it's worth stating here that that regardless of the method of data collection, the tool used to record the data is of critical importance.

> **"Working with Ardoq over the last 12 months has been an eye-opener. The level of insight we get by using Ardoq helps us to understand and discuss our concerns in a meaningful way. Having everything documented and up to date in Ardoq has been a game changer."**
>
> - Capgemini

WHERE SIMPLE TOOLS FALLS SHORT WHEN CREATING DOCUMENTATION FOR GDPR COMPLIANCE:

1. COLLABORATION

Documenting information about the personal data flowing through your organization – from servers and emails, to sales and marketing departments – requires input from multiple stakeholders. Using a tool with in-built collaborative features as standard is far more beneficial than sharing a solitary Excel document and hoping that everyone is using the latest version.

2. AUDIT TRAIL

Being able to access the history of documentation, and acknowledge changes that have been made and the reasons why, can be incredibly useful. If, for example, an auditor uncovers a noncompliant area that you thought you were compliant in, it will be beneficial to be able to track changes to explain what happened, who's responsible, and what can be done to remedy the situation.

3. CLEAR VISUALS

Excel visualizations can be powerful, but without complex customizations and coding interactivity is limited. More dynamic visualizations offer the capacity to explore large datasets, and identify issues or insights that could otherwise be easily overlooked.

4. REUSABLE DATA

If a project is narrow in scope, time, and resources, a one-person team with Excel can go a long way. However, as soon as an element of collaboration is introduced, Excel sheets become difficult to manage. Given the scope of a GDPR compliance project, there will likely be a vast number of Excel sheets created, as well as supporting Word docs and visualizations. Managing file versions in such instances can become a full-time job in itself, and is in no way efficient.

THE DOCUMENTATION PROCESS

By moving project documentation into Ardoq, the client team was able to present a clear audit trail detailing observations, changes, and decisions taken to attain compliance. In the event of an external audit, the team now has the capacity to confidently present this process through interactive visualizations and in-depth descriptions to explain the current situation, as well as future plans on the path to compliance.

IMPLEMENTING GDPR TEMPLATES

Following discussions with the client and its data owners, we developed Ardoq models to answer the key questions they would need to answer on the path to compliance. By documenting the client's data using the GDPR templates, we could quickly visualize and answer the following:

1. What type of personal data is being collected in each process?
2. What is the current assessment of the processes' compliance with individual GDPR principles?
3. Which GDPR principles are most troublesome when it comes to compliance?
4. Which gap observations on application services have the largest impact?

Ardoq AS
Gaustadalléen 21
0349 Oslo
Norway

(+47) 24 02 20 24
contact@ardoq.com
support@ardoq.com

Visit ardoq.com today to schedule an in person meeting with Ardoq locally in

OSLO | COPENHAGEN | STOCKHOLM | LONDON