Defining Success for DSAR Compliance

GDPR Insights

Defining Success for DSAR Compliance

Content Overview

Two Years On, GDPR Remains a Challenge

Since its enactment almost two years ago, GDPR has been transforming the information governance landscape for organizations around the world. While many organizations responded with data privacy policies and cybersecurity rules to adhere to the regulation, it has not been without steep challenges. Many organizations still struggle with compliance, inadvertently overlooking GDPR obligations that leave them vulnerable to severe fines, litigation, and loss of customer or employee trust. In the past 23 months, several organizations have suffered the consequences for non-compliance:

- Marriott International incurred a $123 million fine for exposing 339 million customer records to hackers in 2018.[1]
- British Airways paid $230 million for their poor security protocols which allowed 500,000 website visitors to be redirected to a phony site where hackers could access their personal data.[2]
- Deutsche Wohnen faced a steep €14.5 million fine for not properly disposing of tenant information.[3]
- Google suffered one of the largest GDPR fines of $57 million for failing to obtain consent when collecting and processing user data for ads.[4]

1. CPO Magazine: https://www.cpomagazine.com/data-protection/marriott-faces-massive-123-million-gdpr-fine-for-2018-security-breach/
2. New York Times: https://www.nytimes.com/2019/07/08/business/british-airways-data-breach-fine.html
3. Data Protection Report: https://www.dataprotectionreport.com/2019/11/first-multi-million-gdpr-fine-in-germany-e14-5-million-for-not-having-a-proper-data-retention-schedule-in-place/
4. BBC News: https://www.bbc.com/news/technology-46944696

While most of these are large businesses, it's important to remember that small-to-medium- sized organizations aren't exempt from regulatory fines or litigation. Verizon's Data Breach Investigations Report revealed that 43% of all data breaches involve SMBs.[5] With limited resources and little room for financial error, a GDPR fine (which could total up to 4% of annual revenue or €20M, whichever is greater)[6] could buckle an SMB. A study from consulting firm Switchfast Technologies deduced that within six months of a data breach, at least 60% of SMBs halt business operations.[7]

Based on these numbers, it's easy to conclude that adhering to GDPR data privacy protection rules remains vital to organizations both big and small. But how do organizations measure their progress on the GDPR compliance journey? What constitutes success?

Defining and Achieving GDPR DSAR Success

The journey to regulatory compliance is not simple and is certainly not without significant obstacles. However, any barrier – such as exploding data growth, dark data, and DSAR – can be overcome with investments in process training and enabling technologies aimed at getting an optimal blend of cost and benefit.

5. https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/
6. GDPR.EU: https://gdpr.eu/fines/
7. https://solutionsreview.com/security-information-event-management/switchfast-majority-smbs-go-business-data-breach/

Automating Information Asset Classification and Enhancement

Given the skyrocketing volumes of Dark Data afflicting most organizations, success in this arena from a process perspective is focused on automation. When assessing your organization's level of maturity around GDPR compliance, looking at the degree to which you are automatically discovering, classifying, and governing your assets to proactively identify and remediate PII leakage is critical. Some examples of successful best practices include:

Auto-classification of Information Assets

By leveraging a combination of artificial intelligence, machine learning capabilities, and rules-based approaches organizations can train their discovery products to automatically classify their information assets with a very high degree of accuracy. The classification process can alert data controllers to any personal, sensitive data hiding in unknown or inappropriate locations. Further steps can be taken to move documents, tag them, or to enact tighter access controls as needed.

Automated Named Entity Identification

Named entity extraction can enhance the visibility of data subject information. A specified "named entity" – for example, as a name, location, or organization – can be extracted (based on patterns within the text) from documents, giving exhaustive insight into previously-unknown dark data. Named entity extraction in effect helps to turn unstructured information into structured data that can be efficiently queried to identify rogue PII or other areas of compliance-related concern.

Automated Retention Policy Assignment

Once information has been categorized and metadata enhanced, automated assignment of retention policies is an important step in bringing order from today's information chaos. While 100% automation is not possible, most documents and structured data objects can be associated with appropriate policies through an method that combines machine learning-based training with a rules-driven approach.

By implementing automation, organizations can ensure that information containing sensitive and personal information is identified proactively and protected from any potential misuse as part of an overall information governance regimen.

Scalable and Transparent DSAR Processes

One of the trickier obstacles to navigate around is Right of Access, or Data Subject Access Requests (DSARs). As of late 2019, a Talend survey found that 58% of businesses surveyed struggled to respond to a data subjects' request for information access in the month-long timeframe that the GDPR mandates.[8] As organizations look to demonstrably meet their GDPR obligations related to DSARs, the following criteria provide a good checklist for success.

Automate DSAR processing workflows

Capturing your initial data subject communication should trigger an automated workflow that will set the process in motion. The workflow automation provides process structure and visibility so you can prove you're responding to requests consistently and timely in case of an audit.

8. https://www.talend.com/about-us/press-releases/gdpr-compliance-rate-remains-low-according-to-new-talend-research/

Web-based DSAR request capture and identity verification

Since organizations have limited time to respond to subject access requests, it's imperative to capture requests, verify identification, and answer these inquiries as quickly and efficiently as possible to remain GDPR compliant. Creating a clear channel of communication with data subjects that can trigger the capture and verification process will not only speed up the process through automation, but it can also help prove timely responsiveness to SARs through traceability.

Implement GDPR training for employees

Once you have your automated processes and workflows in place, it's important to provide broad-based GDPR training to all employees. This ensures understanding across the organization of GDPR policies so that everyone is on the same page. Most employees working outside the realm of information governance don't have a full grasp of GDPR and Subject Access Requests and therefore won't know how to respond in case they receive an access request from a data subject through a non-official channel. Furthermore, many employees don't realize that they are GDPR data subjects and that they have DSAR rights that can be exercised with their employer as well as with the companies they do business with.

Measure DSAR disclosure page activity

Just as marketers look at the number of impressions on their website pages to evaluate the effectiveness of their message and strategy, so can data controllers view the impressions of their organization's DSAR disclosure page. Is the organization communicating proactively, consistently, and clearly with customers or clients regarding Rights of Access and data privacy? Monitoring hits on the DSAR disclosure page can reveal the answer to this question.

Track the average turnaround time, handling time, and cost for DSAR responses

·Through a defensible audit trail, a data controller can determine the amount of time it takes to fulfill a DSAR request, calculate the manpower cost of each request, and determine if current processes need honing. Perfecting turnaround time can improve customer service, which in turn can increase customer loyalty, trust, and reputation while reducing the internal cost footprint.

While these may seem like lofty targets at first, they are very achievable for most organizations as part of an overall Information Governance initiative powered by technology solutions like the Information Governance Suite from Nyxeia.

Adopting Data-Driven Monitoring Processes

It may seem like an obvious point, but organizations act smarter and perform better when they are informed by data. Some of the data indicators that can be used to understand if your GDPR strategy is succeeding include:

Number of PII "hits" in inappropriate systems

Are employees storing sensitive information where it does not belong? Do the existing processes involving collection, dissemination, and storage of PII need refinement? What kind of sensitive information is continuously being mishandled, and why? Consistently running PII location investigations highlights problem areas in day-to-day business operations that can be improved upon.

Percent of assets that are correctly auto categorized

Keeping track of this type of data can tell you if the tool's machine learning needs refinement so that manual efforts are spent in more efficient ways.

Volume of information under governance

Upon a first deep discovery dive, an organization will realize that only a small percentage of their information assets are properly governed. The initial discovery unearths large amounts of dark data and ROT that can be cleansed. Once data is categorized, classified, deleted, or archived, the amount of ungoverned data decreases. The focus can shift to newly created content, invariably decreasing security and compliance risks.

The number of systems under governance

Today's organizations are necessarily heterogeneous and combine cloud and premise-based applications from multiple vendors, many containing a wealth of structured and unstructured data. While it is impossible to comprehensively govern all of them immediately, tracking your organization's progress on a system-by-system basis – file shares, email, IM, groupware, structured ERP and CRM apps, etc. – can demonstrate steps toward successful coverage. Federated InfoGov solutions like Nyxeia's Information Governance Suite help organizations build out their system coverage incrementally, one piece at a time.

Tracking and sharing these metrics can help to ensure that your GDPR compliance efforts are well-positioned to remain successful over time, not just as part of an initial push.

Compliance-Enabling Technologies

When looking for technologies to better empower your internal governance processes and achieve the levels of success outlined in this paper, look for tools that enable:

Deep discovery

...to connect to applications housing sensitive information. Sensitive information can reside in many enterprise applications – including groupware, email, instant messaging, file shares, and other places -- even if it is not supposed to. Getting insight into these dark recesses is essential.

Content analytics

...to index, categorize and enhance structured and unstructured information assets to understand their significance and their sensitivity. Armed with a powerful information analytics capability, you'll also be able to better understand where valuable, sensitive, or redundant content accumulates and how to respond appropriately.

Redaction capabilities

...to ensure that information assets, no matter where they live, are redacted for relevant user roles and groups to minimize the potential for an unwanted sensitive data disclosure or breach.

Full lifecycle retention policies

...that model the regulatory, industry, and business-specific requirements your organization needs to enforce and apply them en masse. This capability is really where the true "governance" part of Information Governance comes into play.

Process and workflow automation

...to scale the content categorization effort needed to illuminate the growing volume of data, and to process the flow of Data Subject Access Requests.

Preservation capabilities

...to support the removal of assets from general circulation before defensible disposal or in the context of legal holds as part of an overall information lifecycle management strategy. Preservation activity should be informed by asset retention policies and should be considered a different activity from IT-driven archiving, which is often solely motivated by application cost or performance reasons.

By ensuring that your organization has these tools at its disposal to address the critical business continuity and trust challenges inherent in GDPR compliance, you can help your organization to meet the critical success criteria outlined in this paper.

The Rewards of a Diligent Approach to GDPR Compliance

As much as the topic of GDPR compliance attracts interest from stakeholders across the organization, at the end of the day it is often nonetheless considered a cost of doing business that is easily deferred – at least until a lawsuit or breach makes the importance of these initiatives more readily apparent.

To help your organization be more proactive, it's important to articulate the concrete benefits of GDPR compliance, and of InfoGov overall (a topic of a recent Nyxeia-sponsored webinar with the team at ARMA and leading InfoGov executives).

Some of the rewards associated with GDPR and InfoGov initiative success include:

Reduced Risk of Fines

Reduced risk of non-compliance costs, fines, and litigation. Though the road to compliance isn't cheap, the cost of non-compliance is higher – 2.71 times higher, according to a 2017 Globalscape study.[9] And as of mid-2020, the total amount of GDPR-related fines imposed on companies practicing poor data privacy protection and information governance practices was on the order of €350M – and this will accelerate with CCPA and other state and national regulations currently under development. [10]

Lower Litigation Costs

Poor GDPR compliance translates to poor handling of sensitive data. In today's data privacy protection environment, poor diligence will inevitably carry a cost – potentially a crippling one. Settlements for the likes of Target, Uber, Equifax, and others experiencing PII breaches have neared the $1.5B mark in recent years, and the trend toward aggressive litigation is only growing.[11]

Improved Productivity

Studies by McKinsey and IDC place the time spent by knowledge workers

9. https://www.globalscape.com/resources/whitepapers/data-protection-regulations-study
10. https://en.wikipedia.org/wiki/GDPR_fines_and_notices
11. https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

looking for the information needed to do their jobs at between 25-50% of their workweek.[12] Removing obsolete and irrelevant information as part of an overall InfoGov regimen so that only the latest, approved content is available promises to reduce this figure considerably.

Stronger Revenue Performance and Valuation

In their "Embankment Project for Inclusive Capitalism Report", Ernst and Young "derived a net trust score for a sample of 20 companies on the FTSE, we often found a positive correlation between trust and financial performance."[13] In other words, companies that value good information governance and data privacy protection (and promote this fact) perform better than their counterparts who do not.

Improved Levels of Customer Trust and Brand Loyalty

The advantage of customer loyalty through demonstratable transparency and responsiveness. By taking data protection seriously, organizations increase customer trust, and trust is one of the most valuable assets a company can have for future growth.[14] A recent Gartner Trend Inside Report, Predicts 2020: Barriers Fall as Technology Adoption Grows — A Gartner Trend Insight Report supports this privacy-trust correlation. According to Forbes Insights, 46% of organizations surveyed had suffered damage to their reputations and brand value following a data breach – likewise, those organizations that cultivate customer and employee trust through strong and transparent data privacy protection practices see growth in brand loyalty.

These points illustrate how forward-thinking, compliant, and transparent organizations are leading the way in a rapidly changing information age. As a result, these organizations continue to grow

12. https://blog.xenit.eu/blog/do-workers-still-waste-time-searching-for-information
13. https://www.ey.com/Publication/vwLUAssets/ey-at-embankment-project-inclusive-capitalism/$FILE/EY-the-embankment-project-for-inclusive-capitalism-report.pdf
14. https://adage.com/article/digital/5-key-takeaways-2019-edelman-brand-trust-survey/2178646

amidst a shifting and unpredictable landscape. Every frontier explored is not without potential hazards, but Nyxeia can provide the support your organization needs to traverse the unknown with greater certainty. The Nyxeia team is committed to your organization's success by helping better manage vital information assets, protect sensitive data, and ensure compliance with data privacy regulations. Contact Nyxeia to realize the promise of Insight Reimagined ™.

Find out more about how Nyxeia can help meet the challenge of Data Subject Access Requests

Watch the demo webinar

Contact Us: Info@nyxeia.com

About Nyxeia

Nyxeia provides the industry's most innovative software to help organizations identify their sensitive and valuable information to be more informed, efficient, and compliant with privacy protection regulations. Nyxeia enjoys stable ownership that has for the last 30 years created a portfolio of innovative companies that have become leaders in their markets.