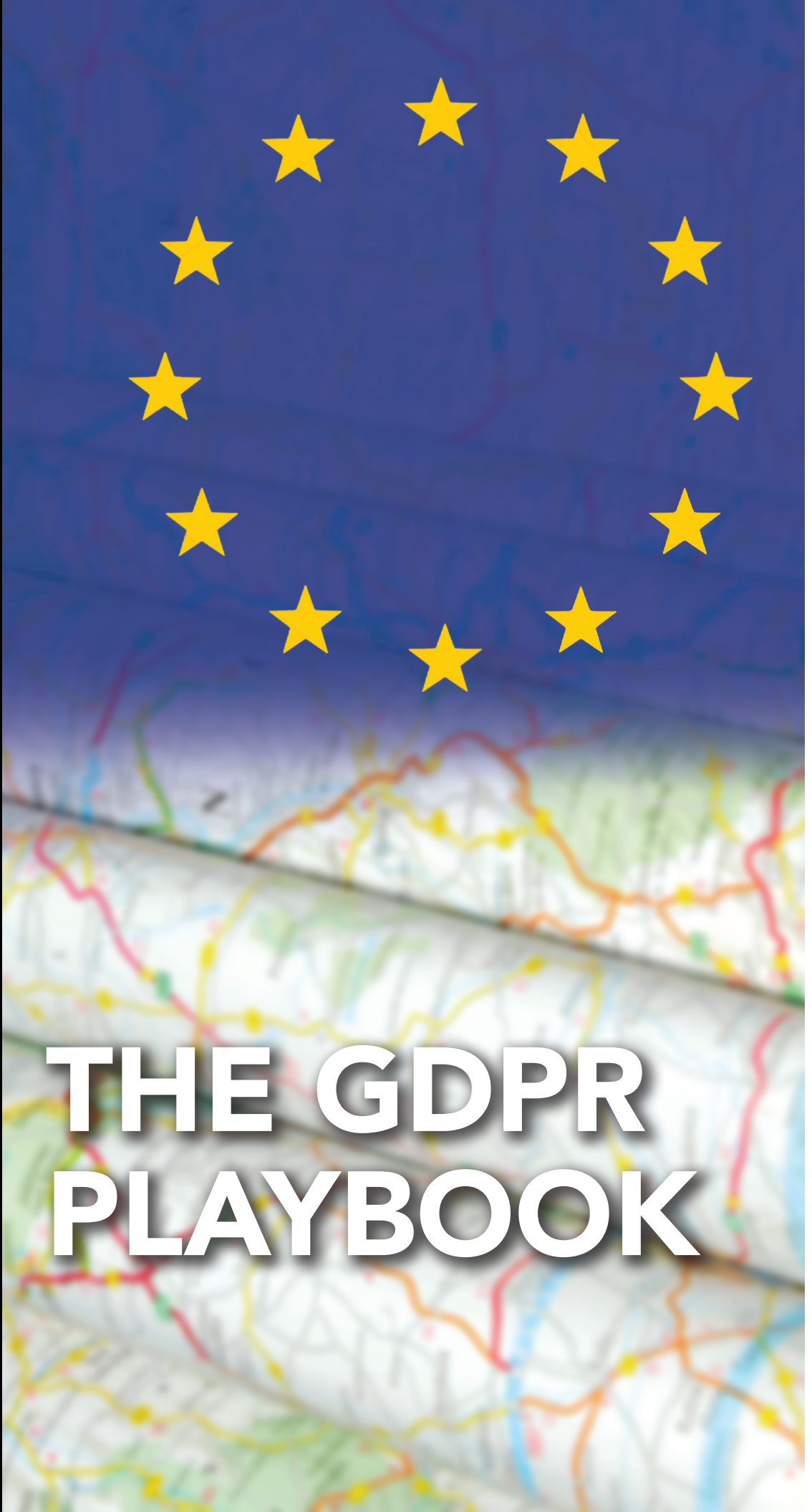

THE GDPR PLAYBOOK

database
TRENDS AND APPLICATIONS

database
TRENDS AND APPLICATIONS
ONE COMPLETE MARKETING PROGRAM

On the Road to GDPR COMPLIANCE

Best Practices Series

The General Data Protection Regulation (GDPR) is coming, and with it, a host of requirements that place additional demands on companies that collect customer data.

While the new regulation has been likened to Y2K because it pushes a hard deadline by which time organizations have to update systems, procedures, and protocols, and because, similar to Y2K, there are dire consequences for those who fail to take it seriously, that is only part of the story.

Y2K prompted doomsday scenarios in which individuals and companies would not be able access mission-critical systems in banking, transportation, and utilities. Many computer programs had previously represented four-digit years beginning with 19 as just the last two digits to save space. It was feared that if January 1, 2000 was indistinguishable from January 1, 1900, activities and events that were programmed by date would have problems and chaos could ensue.

While the "millennium bug" as it was then known was reported to cause some hiccups, the overwhelming majority of companies had taken steps to clear up their issues well ahead of January 1, 2000 with many companies taking long-overdue opportunities to overhaul and modernize more broadly. The day came and went and everyone breathed a collective sigh of relief. People were still able to get cash from banks and gas still flowed at the pumps. The crisis was averted.

However, with GDPR, the looming deadline—May 25, 2018—will just signal the beginning of issues related to the regulation. And, there will be no finite time when companies can be certain that the risk has passed. It will require an ongoing effort to change how data is collected, stored, and governed to ensure that companies are compliant—and stay in compliance.

In an effort to clarify GDPR for those who have day-to-day responsibility for data protection, the Information Com-

missioner's Office, the U.K.'s independent authority, has issued the "Guide to the General Data Protection Regulation (GDPR)."

According to the guide, GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Failure to adhere to GDPR, may result in fines of up to 4% of worldwide revenue or 20 million euros, whichever is greater, making the danger substantial for larger entities.

Among the requirements enumerated in GDPR is that organizations must promptly notify individuals of a personal data breach, within 72 hours of becoming aware of it. Hacking will not be considered an excuse for a breach as companies are expected to take precautions. Companies are expected to have "robust breach detection, investigation and internal reporting procedures in place" and must keep a record of any personal data breaches.

Another one of the more interesting concepts of GDPR is data portability or the ability of an individual to request their data and move, copy, or transfer their data to another service provider or company. And perhaps the most vexing of all is the right to erasure, also known as "the right to be forgotten," which gives individuals the right to have their personal data "erased" and to prevent further use in a variety of specific situations such as when the data is no longer necessary for the original purpose; when the individual withdraws consent; or to comply with a legal obligation.

*GDPR applies to all **companies processing** and holding the personal data of data subjects **residing in the EU**, regardless of the company's location.*

GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location.

This means even if you think you are not doing business with or collecting data about residents of the EU, you had better be sure. And, the only way to be certain is to institute controls about data onboarding, security, unified governance, and access. In this way no matter what new data privacy regulations emerge in any new geographic regions, companies can be sure that, now and in the future, they can pinpoint data across systems and know whose data it is and that they are dealing with every instance of that data.

Will GDPR be the catalyst that changes the handling of individuals' personal data in a fundamental way? Unlike Y2K, that will not become clear on one single day. However, similar to Y2K, GDPR offers the opportunity for companies to make lasting changes that will have a beneficial impact well beyond the specific crisis they are working to avert. ■

—Joyce Wells

BackOffice ASSOCIATES®

Transform and Govern Corporate Data for GDPR Compliance and Long-Term Data Value

The deadline for meeting the General Data Protection Regulation (GDPR) is next month, but the majority of global organizations are still at the beginning of their compliance journey—leaving them exposed to possible high penalties. There is much to understand about the GDPR, and DBTA's GDPR Playbook offers key insights for applying its key tenets as well as sound advice for taking the right steps for proper compliance.

The GDPR is aimed at strengthening data protection rights for European Union (EU) citizens and residents by instituting new security requirements for all organizations—including those without a physical presence in the EU—that collect and process these individuals' personal data. According to the GDPR, personal data includes any data that could be used to identify an individual, including names, addresses, phone numbers, IP addresses, images, videos, and voice recordings (including those recorded via personal assistant services like Amazon Alexa). The bottom line is that the GDPR requires organizations to process all personal data lawfully, fairly, and in a transparent manner. Collected data must be aligned with a specific purpose; not be used beyond that purpose; be limited to only what is necessary for that purpose; and be kept in a form that can be used to identify an EU citizen or resident for no longer than is necessary to serve that purpose.

The new regulation does not mandate a particular solution to achieve compliance, nor a specific set of actions to take to meet its requirements. Instead, organizations must navigate their own paths to determine a suitable roadmap for ensuring personal data is collected and processed with proper protocols for data quality and security. At BackOffice Associates, we specialize in helping companies understand, transform, and govern their data as a corporate asset through trusted information governance and data stewardship solutions. This includes proactively managing personal data to ensure that best-practice data evaluation and protocols are in place for aligning with all elements of the GDPR regulation.

Achieving GDPR compliance requires enterprises to account for where personal data is stored and the nature of that data throughout the business' complex IT system landscape. Whether data is stored in on-premise or cloud platforms or in a combination of both, businesses must deploy a sustainable information governance strategy that aligns with the GDPR regulation and enables the business to leverage its data as an ongoing corporate asset. With the right strategy in place, the GDPR gives organizations an opportunity to transform critical data into an asset that generates tremendous economic value and competitive advantages.

To help organizations lay the foundation for GDPR compliance success and beyond, BackOffice Associates offers an Information Governance for GDPR Compliance Solution, powered by our Information Governance Cloud (IGC) and Data Stewardship Platform (DSP) software products. These tools enable organizations to set, manage and enforce data-related policies.

We also offer a three-phased GDPR-focused engagement that is tailored to each organization's unique business environment and compliance needs. This includes balancing GDPR compliance obligations and organization-specific requirements, maturity, capabilities, and risks; fostering organizational awareness and leadership around GDPR compliance; and creating a fact-based, customized roadmap to ensure ongoing data monitoring and information governance processes.

Through this comprehensive set of software and services, we empower organizations to gain a deeper understanding of personal data by discovering, categorizing, and cataloging it as well as assigning ownership to the data in a security-rich environment. And, with role-based dashboards, information stewards can continuously monitor their systems to ensure the company is adhering to its compliance policies. Additionally, by leveraging a crowdsourcing approach, our solution allows organizations to identify and establish best practices for data management culled from a community of data stakeholders, while embedded machine learning and natural language processing capabilities guide data contributors to create highly impactful governance policies and assets for GDPR compliance needs and beyond.

On behalf of the BackOffice Associates team, we hope you find the GDPR Playbook helpful in your journey to GDPR compliance and are happy to assist with any GDPR questions or requests. ■

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT US AT
info@boaweb.com

BACKOFFICE ASSOCIATES
www.boaweb.com

melissa

GDPR Moves the Match Goalposts

PAST SCV SUCCESS CREATES GDPR FALSE SENSE OF SECURITY

It is widely agreed that GDPR requires a Single Customer View (SCV) for Article 17, the Right to Erasure. Large organizations often have multiple SCV platforms such as Customer Relationship Management (CRM), Master Data Management (MDM), Customer Information File (CIF), Customer Data Platform (CDP), and other fuzzy record match engines.

These platforms have traditionally provided strong success. Therefore, executive management understandably assumes SCV is a completed step in their GDPR compliance roadmap. And, that SCV finds all of a customer's records, despite factors such as nickname variations, different postal and email addresses, typing errors, and other data quality issues.

With GDPR's eye-watering fines, that overconfidence will be an expensive mistake.

BALANCING FALSE-POSITIVE AND FALSE-NEGATIVE MATCH ERRORS

Configuring fuzzy match algorithms of these platforms basically determines the balance point between false-negative errors (incorrectly not matching records) versus false-positives (incorrectly matching records of different people).

Identity data governance is the process of business users and data stewards defining match success criteria, driven by assessment of the business impact of various categories of match errors to align match results with SCV business-use goals. The technical team then executes various match fine-tuning test iterations to optimize the technical configuration of the match engine.

TRADITIONAL MATCH REQUIREMENTS MAXIMIZE FALSE-NEGATIVES

But all traditional SCV systems share a common problem for GDPR compliance—original fuzzy match business requirements are heavily skewed on the side of false-negatives to minimize the risk of any false-positive errors.

EACH FALSE-NEGATIVE IS A GDPR COMPLIANCE RISK

Before GDPR, false-negative match errors could be dismissed as only being minor mistakes that had minimal negative business impact, such as a customer or prospect receiving duplicate marketing messages or analysis being slightly skewed in a statistically irrelevant way.

But GDPR turns that traditional equation on its head. Steve Eckersley, head of enforcement at the Information Commissioner's Office (ICO), succinctly articulated, "What people may think is a minor mistake could lead to the loss of their job, a day in court and a fine."

QUANTIFYING GDPR RIGHT TO ERASURE RISK METRICS

The question is not whether these GDPR platforms have false-negatives, but rather how many. Rough Order of Magnitude (ROM) metrics help quantify the risk as being just thousands of records or possibly millions—each one a potential GDPR compliance violation.

Those risk metrics are vital not only to alert executive management but also to make practical GDPR resource allocation decisions based on ranking and prioritizing the level of risk in these systems.

Good news—you have a number of colleagues that can help, specifically in the field of Governance, Risk, and Compliance (GRC) with titles such as Chief Privacy Officer, Chief Internal Auditor, Chief Compliance Officer, Chief Counsel, and Data Protection Officer (a new position required by GDPR for large organizations). These people are empowered with the authority and budgets to elevate your GDPR risk analysis to the appropriate level.

MEASURING AND TRACKING FALSE-NEGATIVES IS KEY

The GRC professionals will want to review historical metrics such as how many false-negatives are identified month-to-month, how quickly they are remediated, the severity of the business impact, and more. But for most organizations this information is not only unavailable, it is not even being formally monitored in any comprehensive manner.

False-negatives represent a major GDPR-risk blind spot. So it is key to establish comprehensive false-negative reporting and tracking.

SIMPLE TEST: SCV PLATFORM MATCH CONFLICTS

A fast, simple test: Review total customer counts reported by your SCV platforms. Those numbers often differ substantially and can hide surprisingly extensive match conflicts, especially for wealth management and other VIP customer segments which have more records and higher data quality complexity. For example, during a Fortune 100 MDM project, DataDelta's technology determined that a two percent total customer count difference was found to be the net result of match conflicts impacting more than 25 percent of customer source records.

SOLUTION: GDPR MOVES THE MATCH GOALPOSTS

SCV professionals know that simply loosening fuzzy match configurations would cause match results to snowball into useless piles of false-positives. So rigorous fine-tuning iterations must be done like before, but with the goal of erring on the side of false-positives.

The solution may also require augmenting your current SCV technology with more modern, EU-specific data quality enhancements. For example, simply plugging in more sophisticated EU-specific address cleansing and standardization can have a surprisingly significant improvement on the match results. ■

MELISSA
www.melissa.com