WHITE PAPER

# How to Optimize for the GDPR by Leveraging Existing Data

## A White Paper for Executives in Charge of Ensuring Compliance with the GDPR

STIBO SYSTEMS
MASTER DATA MANAGEMENT

Executives often scorn the General Data Protection Regulation (GDPR) for being an impediment. But as this white paper shows, leveraging existing data through data governance and appropriate technology not only ensures compliance with the GDPR but also makes a stronger business case for the company.

## Ubiquitous GDPR

The GDPR, also known as Regulation (EU) 2016/679, is a reality now. The regulation affects businesses and organizations worldwide that process personally identifiable data of their customers, prospects, suppliers or employees. No one is excluded from complying with the GDPR.

In contrast to the previous data protection directive, the new regulation cannot be ignored. Under the old directive, penalties for data infringements typically amounted to €3,000-4,000 – an amount that some companies had even allocated in their marketing budget.

Under the new regulation, the consequences and risks of noncompliance can amount to €20 million or 4% of a company's worldwide annual revenue, depending on which figure is higher. In fact, the GDPR states that "the fines imposed should be effective, proportionate and dissuasive" (Regulation (EU) 2016/679, § 151).

Regarding the dissuasiveness, the exorbitant level of fines has already had a regulatory effect, changing mindsets and practices among companies and organizations worldwide.

## Summary of GDPR

The GDPR was adopted on April 27, 2016, by the EU Parliament and implemented by the EU member states on May 25, 2018. It is the first update of the data protection law since 1995. Since then information technology and the internet have taken giant leaps forward, leaving the old data protection directive (Directive 95/46/EC) behind.

The GDPR requires enhanced protection of personal data of citizens and consumers, which includes specific customer rights that organizations must meet, including:

- Right to be forgotten
- Right to object
- Right to rectification
- Right of access
- Right to data portability
- Consumer consent

Meeting these rights entails an array of consequences for organizations such as:

- On request, organizations will have to delete or complete all data of an individual.
- Organizations can be forced to give insight into what data is being processed and how, and they must be able to exclude individuals from profiling for marketing purposes.
- They must be able to transmit client data to another organization without hindrance.
- They must obtain active consent from consumers to store and use their personal data.
- Data breaches must be reported within 72 hours to authorities, and in certain cases, the infringed individual.

*Noncompliance can amount to €20 million, or 4% of a company's worldwide annual revenue, depending on which figure is higher.*

# How It Affects the CIO

Obviously, large organizations have more data and face a bigger task in optimizing for the regulation. The responsibility of optimizing for the GDPR often lies with the chief information officer (CIO) of the organization.

### Who Is the CIO?

In this context, the CIO is more a role than a title. The CIO is typically accountable for the following:

- IT strategy and planning
- Communication networks
- System operations
- Cybersecurity and risk management
- Software and hardware purchases
- Aligning IT strategy with business strategy

These responsibilities might fall under the chief data officer or IT director as well.

As the overall project manager for the GDPR optimization, the CIO lays out the strategy for GDPR compliance, which involves the following:

- Establishing an organization of data owners and stewards, who can act on an operational level
- Mapping data and making it actionable
- Setting up procedures for quick responsiveness
- Creating transparency

Optimizing for the GDPR requires getting a grip on existing data. While this might entail substantial resources and funding, in general, data governance – including accountability, overview and accessibility – is a good thing. In addition to GDPR compliance, business opportunities also lay hidden in the leveraging of existing data.

# Where Is Data Located?

The problem with existing data is that it often resides in different departments for different purposes and in different formats. The same data sets are often being maintained in different systems without any integration. The result is that no one can pull up the latest version of a personal record.

This is because personal data is often scattered over several domains or stored in silos like email and systems for HR, customer relationship management (CRM), enterprise resource planning (ERP) and customer support.

Although siloed data can be mapped, described and maintained by the CIO's staff of data stewards, it is still a cumbersome process that can contain many errors. Leveraging existing data through data governance can reduce both the workload and the risks.

# Data Governance

Data governance is a comprehensive method, as well as an organizational mindset. It enables people, processes and IT to work together to ensure trouble-free data management and enhance the commercial value of data.

Data governance involves people and technology and cultural and digital change alike. It is a method to leverage existing data and strengthen the following:

- Efficient responsiveness to requests
- Accurate reporting
- General compliance with standards (GDPR, as well as ISO and various industry standards)
- Accountability, stating who is capable of making decisions and responding to change requests
- Company reputation, as data governance helps to avoid breaches and mitigates damages

Additionally, data governance requires a tight focus on three areas: organization, processes and technology.

### Organization

Since the presence of personal data is so pervasive, the whole organization must, to a relevant extent, be aware of how to manage personal data. The GDPR affects every employee at some level.

To create that awareness and change the mindset and culture, CIOs have the task of building a data-savvy organization. They must appoint data owners and stewards who will design policies and guidelines. They must also manage changes for everyone who processes personal data, describe and change procedures accordingly, keep the organization informed and respond to requests.

Accountability is a cornerstone of the GDPR. This includes defining roles and responsibilities, which is an important building block of data governance. The team must agree on the same vision, understand the importance of managing personal data and be highly motivated.

### Processes

The team of data owners and stewards must have knowledge of where data resides and how it can be accessed. This requires well-defined processes.

The second step in leveraging data for the GDPR is to have sound data processes. Data processing can be intimidating. But eventually, we can boil it down to three strategies that work together to create transparency and availability: data mapping, data cleansing and data syndication.

### *Data Mapping*

The CIO's team of data owners and stewards first need to map data to be able to meet requests from consumers and authorities. Personal data often exists in more places than expected: HR, CRM and customer support systems, spreadsheets in personal archives and even emails.

Different departments may maintain their own data management for specific reasons. It is not uncommon to see sales managers maintaining their own private customer files in addition to a corporate CRM system.

Once a clear picture exists of who owns what data, where it is located and flows, how it is labeled and encrypted, how old it is, and what references it has to other systems, then you can start to control and improve the data quality.

### *Data Cleansing*

Cleansing data – immediately following the data mapping – is an important process to secure quality data. A clean data set is free of duplicate information, always updated, and ready for deletion whenever its business rationale ceases to exist.

It is crucial that an organization can extract a complete and updated data record upon request, be it for the sake of transport, correction or deletion. For the same reason, it is critical that the same individual does not exist under different names or addresses in the organization's data storage and processing systems.

Duplicate records are not unusual, considering the number of different data repositories. But in light of the GDPR, duplicates can become damaging because the organization is unable to hand out a complete data record, thus infringing the user's data protection rights. It is also detrimental because the organization might address the user with irrelevant or outdated information, negatively impacting the user's experience and confidence in the organization.

Clean data is both a marketing asset and a necessity for full GDPR compliance.

### *Data Syndication*

Bearing the consequences and the workload of data mapping and cleansing, the CIO should strive for unified and synchronized data processing.

In an organization with many individually maintained data sources and no integration between sources of different departments, there is an increased risk of using personal data that is outdated or incorrect.

The CIO needs a single version of the truth, not an extra silo. While clever data owners and stewards can set up such a record manually by tracking information to the bottom of silos and sifting through servers, this is a time-consuming and manual process.

The need for data governance for syndicated data is increasing in the wake of the GDPR, where you might expect more of the following:

- Citizens exercising their rights
- Authority inspections, planned or ad hoc, motivated by concerned reporting
- Data breaches as a result of malicious attacks

If you want to achieve efficient data processing, strengthen responsiveness and minimize risk, then automated data syndication is the answer.

## Technology

Even with a data-responsible staff in place and a detailed map of where data resides and flows, it is not feasible to visit several systems and files to meet a simple request.

Stibo Systems provides technology that can help to automate data processing. A master data management (MDM) system is a centralized repository for data that creates a single version of the truth, making it readily available and always up-to-date for anyone in the organization.

## The Golden Record

The golden record is the visible result of an MDM system that unifies and consolidates data from different data silos and creates a single, updated customer view. The MDM system can either break down silos or coexist with them.

The organization will then have a single entry point for retrieving personal data, enabling faster responses and accurate records. The algorithm of the MDM system identifies duplicates and incomplete data by comparing it to data from other sources.

*The CIO's best friend in optimizing for the GDPR is a data repository that centralizes and consolidates the organization's existing personal data.*

Stibo Systems MDM integrates data from multiple systems to cleanse, validate and map source formats to specific data models, along with both probabilistic and deterministic matching and linking to validate incomplete or conflicting data.

As a result, data officers can pull down all relevant data, updated and of high quality, whenever needed, whether for GDPR or commercial purposes.

In short, Stibo Systems MDM provides:

- Flexible data models to support complex requirements and relationships between domains and hierarchies
- Clear ownership of data that enables data governance policies and processes, including audit trails, version control and approvals, along with integrated workflows and business rules
- Data syndication to efficiently deliver master data to multiple stakeholders or channels
- Powerful matching, linking and merging functionality for identifying and handling duplicates and conflicts
- Precise identification of erroneous customer data with strong profiling, cleansing and enrichment
- Dynamic visualization to easily view relationships between products and navigate to linked master records

At Stibo Systems, we are dedicated to helping customers keep pace with evolving trends and regulations.

## Leveraging Data Is Key to Commercial Success

Now more than ever, commercial success is dependent on data collection and the use of existing data. This is why compliance with the GDPR is a competitive advantage.

The GDPR has raised the bar concerning data protection and processing, and the new regulation has a compelling effect on businesses to cleanse and leverage their data. Thus, the GDPR plays into the hands of large companies by offering them an extraordinary opportunity to use the same data for commercial purposes as well.

Exactly at this point, a Stibo Systems solution can tap in and help to leverage data for compliance, as well as to drive better business outcomes. A Stibo Systems MDM solution:

- Acquires, manages and publishes data to support digital transformation
- Offers a multidomain solution that can expand to other domains (customer, supplier, location and employee) without added integration, providing a single version of truth for enterprise master data

Given the extensive storage and consumption of employee and customer data in businesses, there is a huge potential for both cost reductions, business streamlining and enhanced customer experiences if that data is leveraged correctly. Almost every company has unexploited personal data. The GDPR does not forbid the use of personal data; the regulation sets the terms right and prevents unjust exploitation.

In the case of the GDPR, legal demands and business goals pull in the same direction. When businesses undertake data governance and apply automated data syndication powered by an MDM system, you will see palpable commercial side effects to the GDPR compliance, such as:

- A 360° view of the customer, which is a good foundation for providing better customer support
- Reduced manual processes, thus freeing human resources for more revenue-generating activities
- Data quality that ensures an optimum customer experience
- Better targeted use of commercial material, (e.g., in case a user changes marital status, becomes a home owner, etc.)
- Brand building: GDPR compliance is a quality stamp in the internet age, where trust has become one of the most important assets

Fragmented and duplicated customer data residing in siloed systems confines a company's ability to act quickly and grow. Mastering customer data and integrating it into essential business systems for transaction and analysis unlocks the potential value of data.

To learn more about how to optimize for the GDPR by leveraging existing data, visit **stibosystems.com** or email **info@stibosystems.com**.