WHITEPAPER

The Right To Be Forgotten (RTBF)

An Enterprise Automation Challenge

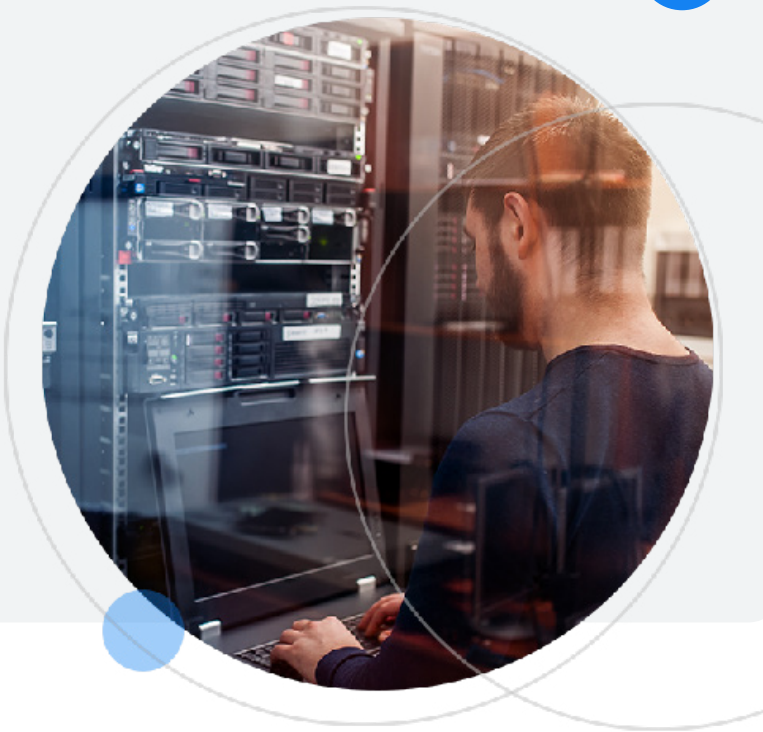
Individual data and the right to be forgotten

Since the enactment of the European Union General Data Protection Regulation (GDPR), the pace of new data protection legislation and amendments has increased around the globe. One core principle guiding this wave of regulations is who has the right to control personal data. Shifting the balance, it is now up to individuals to determine if and how a business can use their data.The business, on the other hand, is responsible for protecting personal data that has been entrusted to their care – whileaddressingindividual wishesand complying with multiple regulations.Enterprisesare, therefore,boundby law toabide byconsent permissions, consumer rights requests, and security standards.

While data protection laws have some variations with consumer rights requests, there is broad consensus that every person has the right to:

- Access and receive a copy of their personal data
- Update inaccurate or incomplete personal data
- Limit the use of personal data
- Reuse personal data by providing it for other services
- Erase or anonymize personal data – also known as the right to be forgotten

Complying, in a timely manner, with data rights is a challenging undertaking for data-intensive enterprises. But the right to be forgotten may be the toughest of all.



What makes the right to be forgotten so challenging

A typical enterprise has dozens, or hundreds, of data systems — deployed on disparate on-premises and cloud environments—across which customer data is fragmented. This mass-scale, complex IT landscape makes it challenging for many enterprises to comply with individual rights requests, especially due to the time constraints stipulated by the legislators.

When it comes to the right to be forgotten, the challenges are compounded. Before erasing something, you need to know where it is. However, discovering personal data, which is also required for complying with other consumer requests, is just the beginning. Other industry regulations can determine what you are allowed to erase, and company policies oftenrequire stringentchecks and approval processes. Furthermore, erasing data from onetable, orsystem, can have adverse effects on data integrity in another table, or system. Deletingan individual's data is an intricate, delicate process.

Let's take a closer look at key challenges enterprises facein responding to deletion requests.

Key challenges

Discovering and collecting the data

The first step is to find the individual's personal data, which may be scattered acrossmany enterprise systems. Once this information has been located, many enterprises include a collection step enabling privacy and legal professionals to examine the data prior to taking irreversible deletion actions. Collecting this data can be a time-consuming process that involves tickets to the various systems and the involvement of relevant IT teams. In addition to the time this process takes, as more employees get involved in the process of extracting production data, there is a growing concern that personal data will be wrongfully exposed.

Defining the deletion process

Before the deletion process can begin, it is important to determine if specific data can be erased, or whether other laws require a longer retention period. In such cases, only some of the data can be deleted. The response to the RTBF request mustindicate, what data cannot be deleted and the legal basis for this provided to the requesting individual.

Once the deletion process begins, the order of deletions is of the utmost importanceto ensure data integrity.This requires understanding the customer data structure and connectivity within each system and between multiple systems. Furthermore, since this process requires multiple steps across multiple systems, it needs to build in recovery and roll back steps in case of failure.

The mechanics of deletion

With the deletion process defined, it's time to take a closer look at the act of deletion. In the case of manual processes, data engineers must access each system individually,which is time consuming, error prone, and risky in terms of exposure of personal data. Alternatively, automated processes must be able to connect to each system and access the required data. In the diverse enterprise landscape, some systems allow direct connections, some require API-based integrations, and emailnotifications, etc.To compound the complexity, certain systems provide limited maintenance windows for executing these operations.

Depending on the specific privacy law, data anonymization can be implemented instead of actual erasure. This task requires the integration of data masking functions that can replace real data with realistic yet fake data. When anonymizing an individual's data, it is critical to maintain the referential integrity across tables and systems as well as to ensure consistency of the masked values.

After the entire process has been completed, verifying the complete deletion is an additional, crucial step. This validation process should be executed several times to ensure that the data has been completely and permanently removed.

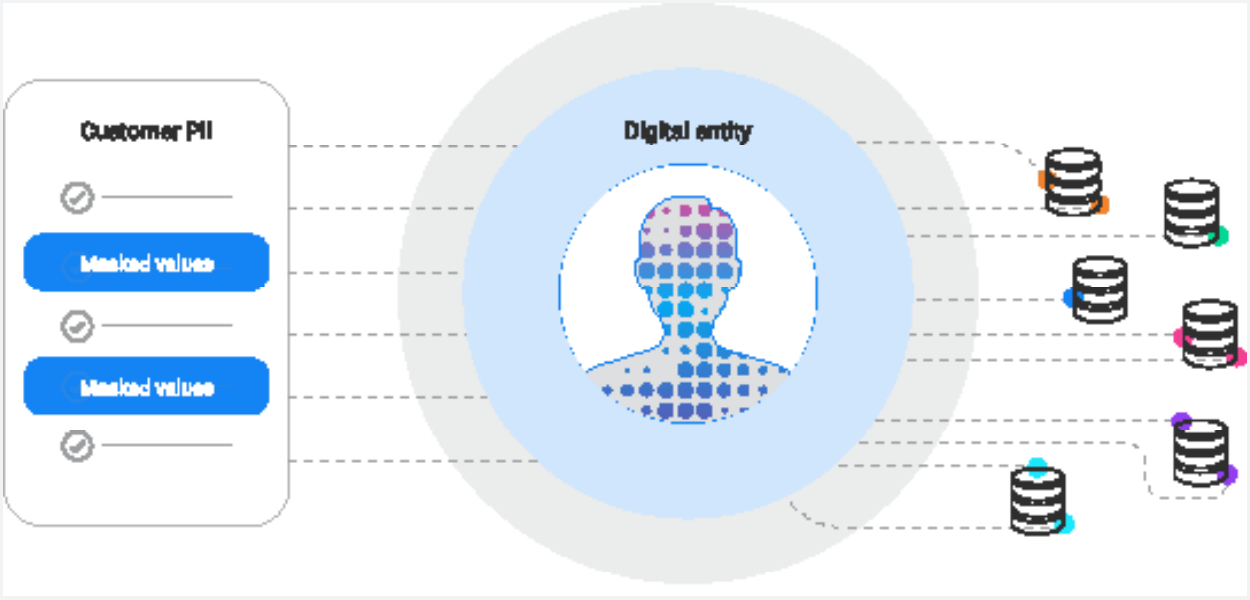
Enabling the Right to be Forgotten with K2View

Most data privacy software solutions automate Data Subject Requests (DSRs) processes, but leave data processing – accessing, collecting, updating, and deleting– to manual, time-consuming, and error-prone human intervention.K2View Data Privacy Management streamlines the DSR workflow, andthe data processing,by maskingall Personally Identifiable Information (PII). With fast, fully documented responses to DSRs, including erasure requests, enterprises accelerate trust and ensure compliance.

Entity-based approach

K2View Data Privacy Management is based on the company'sData Fabric, which organizes fragmented data from disparate systems according to Digital Entity™ data schemas – like customer,employee, etc.

The digital entity unifies all the private and sensitive data that a company know about an individual – across all enterprise systems. Theorganization ofa person'sprivate data intoindividualdigital entities, is uniquely qualified for protecting individual data privacy rights.It simplifies data classification, and data retention management – and also provides security at the entity level, virtually eliminating the risk of mass breaches.



Automated orchestration

K2View provides an intuitive graphical tool used to design data movement, transformation, and business-flow orchestration. Featuring a powerful user interface for creating and debugging business and data flows, it also provides a high-performance execution engine that orchestrates complex processes and data movements.

The entity data schema provides the blueprint for an individual's private data. Based on this information, the deletion process can be carefully orchestrated across all systems.

Data masking tools

Using graphical data orchestration, K2View data masking can be integrated into complex anonymization processes across multiple systems.

The entity-based data model simplifies the complexity ensuring that individual's personal data can be anonymized consistently, across all sources, while preserving full referential integrity.

Built-in enterprise connectors

After years of providing comprehensive data fabric solutions to some of the world's most data-drivenenterprises, K2View has developed a broad library of built-in connectors. These connectors, coupled withour experienced team of data architects, accelerate implementation of complex data-intensive projects.

Summary

With the increase of data protection regulations, companies are forced to take a closer look at their ability to respond to people's data requests in a timely manner. For data-intensive enterprises dealing with complex disparate IT landscapes, these requests in general and especially the 'right to be forgotten' pose significant challenges.

To address these requirements at enterprise scale, K2View's unique Data Privacy Management provides a powerful solution. The solution's entity-based approach is ideally suited for enterprises with complex and diverse IT systems that want to effectively accelerate responses to individual rights requests. Our data orchestration and data masking enable enterprises to simplify and streamline users' erasure requests with end-to-end automation of the right to be forgotten.

To find out more, we invite you to visit our website.