RIXON TECHNOLOGY

SECURITY BY DESIGN:
Defending our clients by protecting their clients

RIXON

VAULTLESS TOKENIZATION AND THE RIGHT TO BE FORGOTTEN

Regulations like the GDPR and CCPA mandate a consumer's "Right to be Forgotten" (RtBF). Such laws potentially create security issues, add administrative overhead, and increase a company's audit burden. Tokenization, particularly vaultless tokenization, offers a workable solution to the RtbF conundrum. Rixon Technology's vaultless tokenization solution enables a simple way to implement the RtBF requirement. Rixon achieves this by transferring control to the consumer over his or her personally identifiable information.

INTRODUCTION

The EU's General Data Protection Regulation (GDPR) and comparable American statutes like the California Consumer Privacy Act (CCPA) require companies to extend a "Right to be Forgotten" (RtBF) to consumers. This right enables a consumer to request that a company with whom the consumer has done business to delete the consumer's personally identifiable information (PII) from its databases. Such a request seems simple in theory, but in reality, it's much more complicated. The RtBF potentially creates security issues, adds administrative overhead, and increases a company's audit burden.

Tokenization, particularly vaultless tokenization, offers a workable solution to the RtBF conundrum. Rixon Technology enables an administratively lightweight, secure, and auditable way to implement the RtBF requirement. Rixon Technology achieves this by transferring control of the consumer's personally identifiable information to the actual data owner (the consumer). Also, Rixon's unique RtBF process can be reversed if the consumer wants to be "remembered" in the future.

THE **BUSINESS IMPLICATIONS** OF RIGHT TO **BE FORGOTTEN**

Laws such as the CCPA and the GDPR went into effect as of 2018 and 2019, respectively. Such laws aim to protect consumer privacy by requiring companies to disclose personally identifiable information (PII) collected from a consumer.

Many companies are still grappling with the implementation of privacy rules such as the CCPA and GDPR. For instance, the CCPA states, "A business that receives a verifiable request relating to the above is obligated to delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records." This concept is evident in theory, but the actual implementation can be challenging to execute and can result in unexpected costs and other difficulties.

First, there's the data management process of determining which information collected from a consumer constitutes PII. Then, a company must identify which received data is potentially subject to the RtBF. For example, if Mary Jones (the "data owner") buys a pair of size 9 shoes, Mary's name is PII and is subject to the RtBF, but her shoe size is not and may be retained by the company.

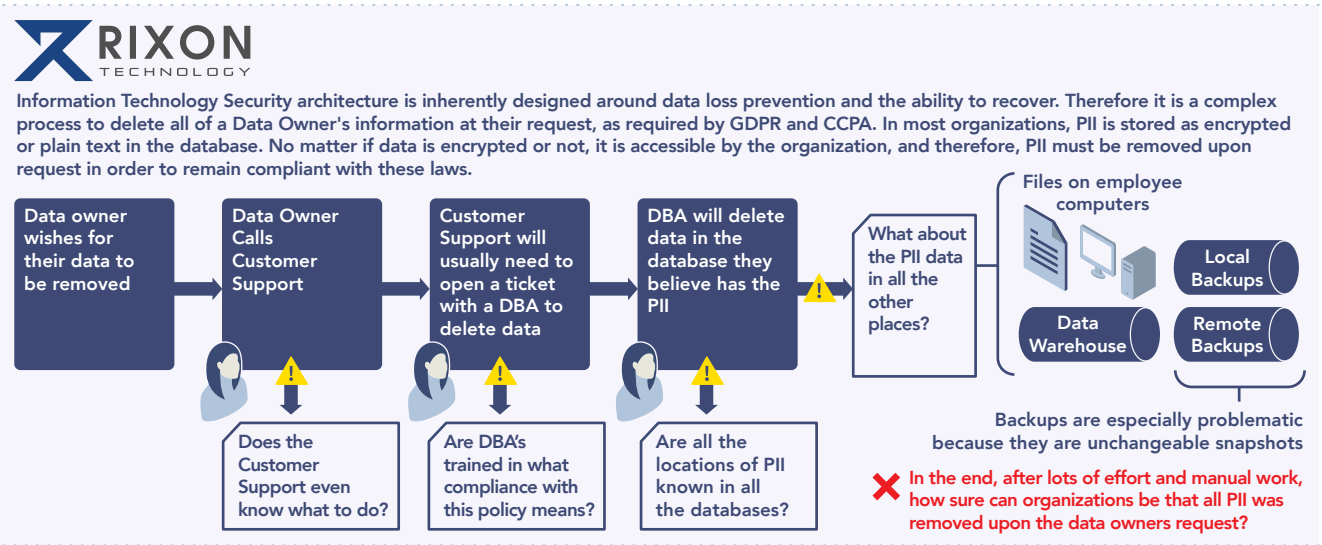


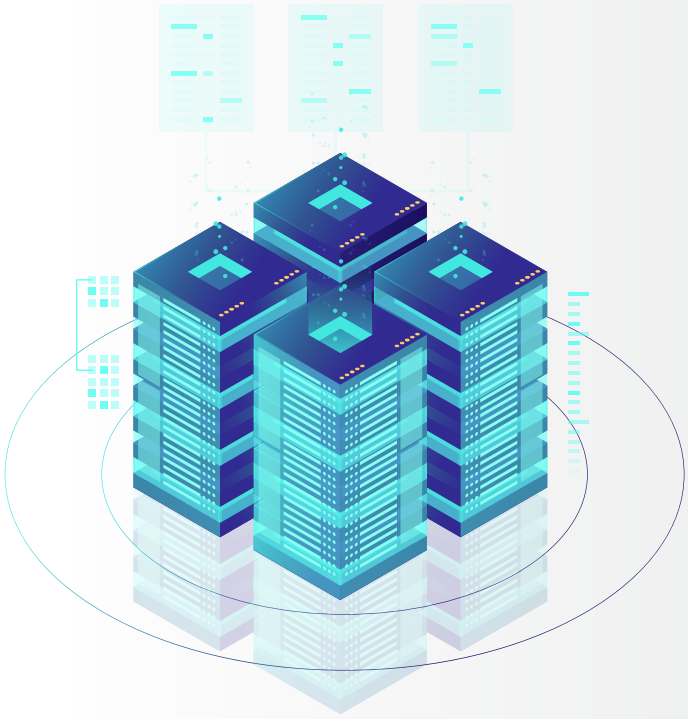
Figure 1 - The standard approach to RtbF, which relies on customer support calls, service tickets and human DBAs executing the process.

Figure 1 depicts the process currently in use for RtBF in many organizations. Under this typical scenario, Mary Jones calls the company and speaks with customer support. She requests that her data be deleted. DBAs executing the process.

In other words, she wants her PII to be "forgotten" by the company. The customer support representative creates a service ticket that goes to a Database Administrator (DBA). The DBA then manually purges Mary's data from the database.

There are several problems with this approach to the RtBF. Most importantly, this typical process can be costly and highly inefficient. Moreover, while well meaning, these processes may fail to follow the law in sufficient detail to make the company compliant with the requirements of regulations such as the CCPA and GDPR. If a DBA does not know where to look or inadvertently overlooks relevant databases, he or she may accidentally do an incomplete RtBF. Thus, Mary's PII could still be lurking in multiple databases within the company. This kind of well-meaning but non-compliant RtBF process can leave the company unexpectedly out of compliance with the CCPA, GDPR, or related laws. The consequences might include fines, penalties and even brand damage.

Data backups and data warehouses present additional compliance risks. An extensive database full of PII can be a treasure trove to a hacker or other unauthorized party. Under the CCPA and similar laws, a PII breach can result in legal liability as well as high costs, driven by consumer notification requirements. The brand may also suffer reputational damage. Fines of between $100 and $750 per consumer can also be imposed on the entity suffering the PII breach. Doing the math, the breach of a 100,000-record PII database could cost between $10 and $75 million in costs and fines.



To guard against such substantial financial impact from a data breach, many companies currently encrypt their customer data. While encryption is a standard security measure employed by many companies, this approach is not optimal and possesses vulnerabilities. For instance, if a hacker or unauthorized party obtains the encryption key, the data is now subject to exposure. When data is encrypted, complying with an RtBF request involves the cumbersome and insecure process of decrypting data to confirm possession of PII. Only then can the company proceed to delete the PII. Some organizations address this problem by performing the RtBF requests manually. In doing so, however, companies are faced with a costly, time-consuming, and inefficient overall process.

THE RIXON SOLUTION APPROACH TO THE **RtBF**

The objective for most, if not all, companies subject to the CCPA, GDPR, and comparable regulations is to be able to perform an RtBF request as efficiently as possible. Thus, the fewer manual steps, the better. Auditability is also essential.

The Rixon Solution provides a patented, vaultless tokenization solution that meets these criteria and more.

Understanding Vaultless Tokenization

Traditional tokenization uses a process in which the service provider stores customer data, creating an administrative burden and a security risk. With vaultless tokenization, the service provider only stores the tokenized data.

In other words, vaultless tokenization realizes the process without requiring the merchant, or "service provider" organization to store the original data in a digital "vault" on its premises.

As depicted in **Figure 2,** when a consumer/data owner initiates a transaction with a service provider, the Rixon Solution converts the consumer's PII to format-preserving, smart tokens. Rixon transmits these tokens to the service provider, who then stores the tokens (not the actual PII) in its database. When needed, the Rixon Solution also enables the service provider to de-tokenize a consumer's data in order to complete a payment card or banking transaction, or any other necessary business tasks.

ENCRYPTION VERSUS TOKENIZATION

Encryption and tokenization are similar in that they both protect data by making it unintelligible to people who lack the means to decipher it. Encryption achieves this result using a mathematical encryption algorithm and related key to transform plain text into cipher text. Thus, the social security number 143-87-9234 can become the cipher text 76194404036996692953.

Tokenization, in contrast, replaces data with randomly generated token values for plain text and stores the mapping between the token and actual data in a database. With format preserving tokenization, a social security number 143-87-9234 might be tokenized to become 434-03-0792. Thus, with tokenization, the data format is maintained without diminishing the strength of security.

The Process

Secure & Seamless

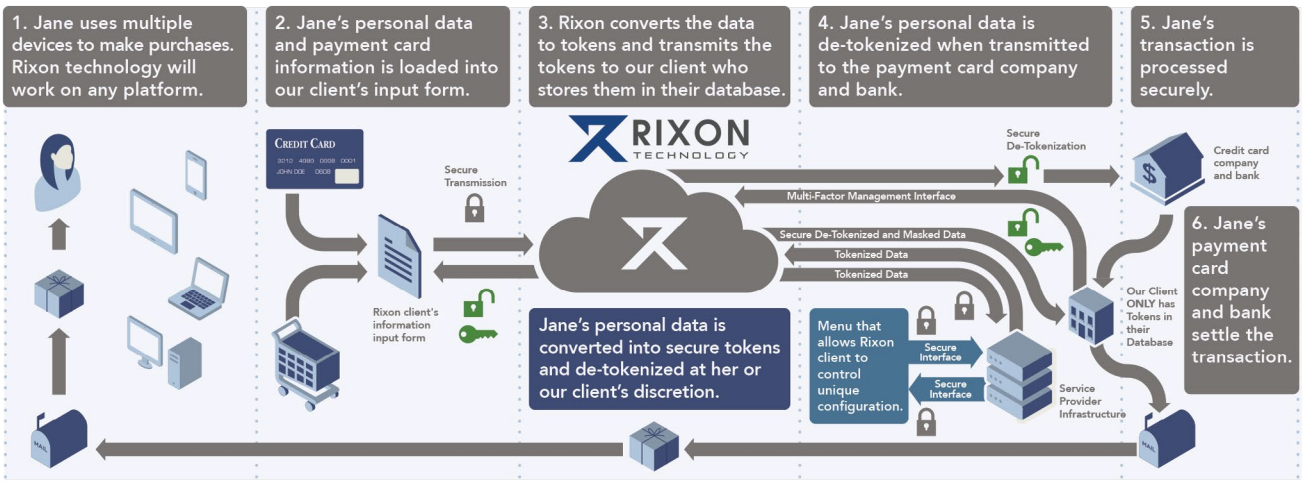


Figure 2 - Reference architecture for the vaultless tokenization process.

HOW THE **RIXON SOLUTION ENABLES** A STREAMLINED, ADMINISTRATIVELY LIGHT **RTBF PROCESS**

The Rixon solution provides a streamlined, administratively light mode for satisfying the RtBF requirements of applicable laws. As shown in Figure 3, this process starts with the service provider using a multi-factor authentication (MFA) process to establish that the actual data owner has initiated a data deletion request. The Rixon Solution also enables a geo-fencing of the RtBF process. For instance, if a data owner requests access from outside a permitted area, the Rixon Solution can be further directed to deny it.

The consumer ("data owner") then uses a simple Allow/Not Allow toggle button in the user interface to trigger the tokenization process of their PII. If the data owner selects "Not Allow," their PII is tokenized and masked from the service provider. While in this form, the tokenized PII is not stored in un-tokenized form anywhere on the service provider's infrastructure. If an employee of the service provider attempts to look up the tokenized part of a consumer's record, he will only see tokens. Further, even Rixon Technology cannot view or access the consumer's tokenized PII. It is "forgotten." As long as a consumer's unique Identifier is not present, the service provider may not de-tokenize (i.e., may not view) the consumer's "forgotten" PII. Thus, once the data owner has performed the RtBF process using his or her unique Identifier, the service provider can no longer see the PII. It loses the ability to de-tokenize the data. The entire RtBF process happens automatically and transparently. No employee at the service provider has to do anything to fulfill this RtBF request. The consumer/data owner is provided with control of the process by interacting with an online user interface.

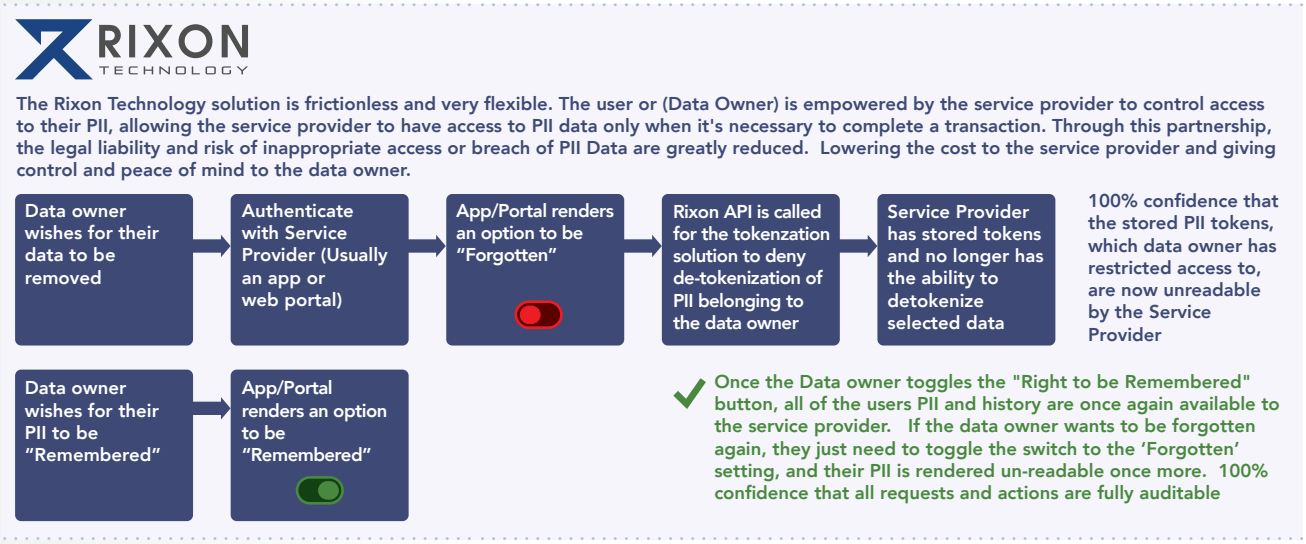


Figure 3 - The RtbF process, using the Rixon vaultless tokenization technology

Configurability

The Rixon RtBF feature is entirely configurable, just like the Rixon tokenization solution, including menus for audit and tracking that the service provider can configure to match business tracking needs. For instance, the Rixon Solution can be configured to separate PII from bulk transactional or inventory control data that the service provider needs to keep (e.g., shoe size) for business-related, administrative, and inventory needs.

Auditability

The Rixon Solution RtBF process is also entirely auditable. The fulfillment of an individual consumer's RtBF request is fully viewable by an auditor. At a higher level, the auditor can also confirm that the Rixon Solution provides a viable, administratively simple path to the RtBF—thus proving that the service provider is complying with the CCPA, GDPR, or other applicable laws. The process is easy for auditors to understand and verify through automatic logs creation, enabling quick spot checks by auditors for RtBF compliance.

Additional Benefits

In addition to configurability and auditability, Rixon's patented vaultless tokenization approach to the RtBF process offers other business benefits. As an automated process, it moves quickly and enables a fast, satisfactory resolution to a customer's RtbF request.

The process does not require employees to manually do the work, saving money, and avoiding errors in the process. The process is also transparent, seamless, and customizable. As a result, compliance with the CCPA, GDPR, and related laws is simplified, and relevant compliance and audit costs are reduced.

THE RIXON SOLUTION

The Rixon Technology solution is a patented, cloud-based security solution that consists of a vaultless, format-preserving, smart tokenization, multi-lingual process. It is also high-speed, seamless, customizable and offers unlimited scalability that is unmatched. And, it is completely transparent to the authorized user or application.

Through the Rixon Solution, an organization can replace raw PII data with tokens that are uniquely configured to meet security and risk tolerance requirements. Only authorized individuals and applications will have access to secured information through a multi-factor process.

REVERSIBILITY AND THE **“RIGHT TO BE REMEMBERED”** (RtBR)

The Rixon Solution also makes RtBF reversible. In other words, not only can a consumer’s PII data be “forgotten,” but it can also later be “remembered.” Similar to the RtBF process, to be remembered, the consumer (“data owner”) need only to return to the same RtBF interface and toggle the button from “Not Allow” to “Allow.” Solely the data owner controls this “Reversible Masking” process.

The Rixon RtBR feature allows a company to offer a data owner the ability to return to a merchant’s environment at a later date without having to re-establish their account information with the organization again. Through reversal of the “Allow/Don’t Allow” toggle button, the data owner can easily make his or her data visible or invisible to the service provider as often as needed for current and future transactions with a particular merchant or business. The net effect of the RtBR feature is to reassure the data owner that their PII will not be exposed to theft in a data breach during periods when the consumer is not conducting business transactions with a company. Similar to the Rixon RtBF feature, the Rixon RtBR feature also compresses data security and compliance costs, and further compresses the service provider’s data breach vulnerability footprint.

BROADER SECURITY AND COMPLIANCE **BENEFITS** OF THE RIXON SOLUTION

The Rixon vaultless tokenization solution provides security and compliance benefits that extend beyond valuable RtBF and RtBR features. For one thing, the Rixon Solution reduces an organization's security attack surface area and compliance footprint. This occurs because the cloud-based, vaultless tokenization solution enables the service provider to store no actual PII on its databases. For the hacker or an unauthorized party, there simply is nothing to steal. Instead, a breach of the database will only yield useless tokens.

Self-Healing Process

One notable aspect of the Rixon Solution is its utilization of an isolated, self-healing, immutable infrastructure to handle the tokenization and de-tokenization process. As a result, even Rixon Technology does not have nor require access to the server environment. The design makes it virtually impossible for a malicious actor to penetrate the environment and access de-tokenized data.

Business Continuity

One notable aspect of the Rixon Solution is its utilization of an isolated, self-healing, immutable infrastructure to handle the tokenization and de-tokenization process. As a result, even Rixon Technology does not have nor require access to the server environment. The design makes it virtually impossible for a malicious actor to penetrate the environment and access de-tokenized data.

Data Access Visibility

Data access visibility is a further security benefit of the Rixon vaultless tokenization Solution. The service provider can use the Rixon Solution to identify which users have access to specific data. This visibility includes access logs that report on the date, time, and location of access sessions. The solution also provides continuous monitoring of data access and reporting on how users are interacting with tokenized data and related processes. These capabilities are useful in digital forensics, audits, and incident response. Security analysts will benefit during and after a breach from knowing who had access to tokenized data, when the access occurred, and under what circumstances. If a violation of an organization's servers has already occurred, data access visibility can help forensic analysts determine the root cause of the attack.

Compressed Audit & Governance Scope

The Rixon vaultless tokenization Solution compresses the scope of audits and governance. With encryption, every part of the infrastructure, applications, and people typically fall within the scope of regulatory governance and audits. In contrast, the Rixon Solution removes much of the IT environment from auditor's sphere of interest. Once the data is tokenized with the Rixon Solution, the tokenized data does not present a vulnerability to security or compliance. If a hacker or unauthorized party gains access to or steals such tokenized data, there is no consequence. The tokenized data is useless; thus, the protection of worthless tokens is not an auditable concern.

Conclusion

Privacy laws like the CCPA and GDPR are here to stay, and likely to become stricter and more pervasive in the future, with numerous states in the US and countries around the world expected to adopt similar standards soon. At the same time, the need for data security grows more intense with every passing year. These two factors make the Rixon vaultless tokenization Solution an appealing option for the protection of PII.

The Rixon Solution makes it possible to fulfill the RtBF requirements of the CCPA, GDPR, and related laws without resorting to an inefficient or less-than-ideal security solution. The data owner is finally in control of confidential, valuable PII data through automated, seamless, lightweight RtBF, and RtBR processes. Such features provide substantive cost savings and positive brand experiences for a company and its consumers (data owners). Moreover, the RtBF and RtBR processes are reversible only by the data owner. The data owner has control, choice, and flexibility regarding who can view his or her PII and when. More broadly, the Rixon vaultless tokenization Solution enhances an organization's security posture by reducing a company's audit footprint and compliance burden at the same time.

The Rixon Solution offers a combination of advanced vaultless tokenization, and RtBF and RtBR features, that provide access for an organization to a very forward-thinking approach to information security and compliance. Through the Rixon Solution, an organization can simultaneously free its resources and revenue while taking more definitive control of their cybersecurity posture. The positive financial impact and Return on Investment from the Rixon Solution's utilization are quite impressive, with some organizations seeing a potential 34% to 42% drop in security and compliance costs.