RIXON TECHNOLOGY

SECURITY BY DESIGN:
Defending our clients by protecting their clients

RIXON

SOLVING THE RIGHT TO BE FORGOTTEN AND OTHER USER RIGHTS ISSUES

RIXON TECHNOLOGY offers a patented cloud-based security solution that enables an organization to secure its data from unauthorized access. This state-of-the-art security solution offers access to a vaultless, format-preserving, smart tokenization process that is high-speed, seamless, customizable and scalable. The Rixon Technology solution is also completely transparent to the authorized user or application. Through the Rixon Technology solution, an organization can replace raw data with tokens it has uniquely configured to meet its security and risk tolerance requirements. As a result, only authorized individuals and applications have access to secured information through a multi-factor process.

Data protection legislation was originally about protecting personally identifiable information (PII) from hackers. Following GDPR, it is now also about protecting PII from misuse by business. This is achieved by giving users control over the use of their personal information even after it has been collected by business, and even if they gave consent for it to be collected.

> **GDPR gives users eight specific rights over their data.** Five of these impose required actions by the business at the request of the user: the right to access the PII being held; the right to correct any errors in that data; the right to have that data deleted (that is, the right of erasure, more commonly known as the Right to be Forgotten); the right to restrict processing of the data; and the right to avoid any automated decision-making based on that data.
>
> The best known of these – probably because it is widely considered to be the most problematic – **is the Right to be Forgotten (RTBF)**. However, it is worth noting that any solution to RTBF will most likely solve the other four issues since the business difficulties are similar – locating and handling individual user records wherever they occur.

The user rights movement started by GDPR is spreading around the democratic world. It has been adopted in Brazil (LGPD) and will be adopted by California's upcoming California Privacy Rights Act (CPRA). CPRA will affect PII collected after January 1, 2022 and will take effect from January 1, 2023.

User rights over the use of their personal data will undoubtedly spread further, both at U.S. state level and international level around the world. In all existing cases, these user rights apply to both resident organizations and non-resident companies doing business locally. The combined size of the European and California markets is huge, and almost all companies are or will be subject to user rights and the Right to be Forgotten.

The Right to be Forgotten

GDPR Article 17	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay
CPRA Sec 5	A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.
LGPD Article 18	[Data subjects rights include] anonymization, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of this Law

THE RTBR **problem**

PII is ubiquitous within business. It is basically 'customer information'. RTBF requires that every instance of PII should be available for deletion on demand. But most companies don't know where it is held. It could be in databases; it could be free form in emails and letters; and with the rise of remote working, it could be on employees' home computers in spreadsheets or in their Shadow IT cloud apps.

The cost of tracking all this data, or locating it for deletion when necessary, is high. The cost of failing to fulfil a lawful deletion demand is equally high.

But there is a further problem. Users have the additional right to take private action against companies that do not comply with their legal rights. In Europe, one of the primary privacy activists, Max Schrems, has an organization called None of Your Business (NOYB). NOYB helps individuals or groups press their claims against companies. Furthermore, in a litigious country such as the U.S., the right to private action is like a blank check to the waiting lawyers.

Further, the potential for activist groups to organize large scale simultaneous RTBF demands from hundreds or thousands of similarly minded activists could be a hammer blow to targeted companies.

The only solution to the RTBF problem is to be able to fully comply with the RTBF requirement. The same applies to the other rights conferred on the user. The question is: **How can this be achieved?**

THE Rixon **solution**

Rixon Technologies is a tokenization company – but one with a difference. The tokenization engine is held within immutable cloud servers which no-one – not even Rixon – can access. It is a vaultless, cloud-based, high-speed, patented tokenization of immense complexity. If the tokenization engine were compared to the German Enigma machine of WW2, this one would comprise a million wheels (the four-wheeled Enigma was never cracked). But it is also hugely configurable. The tokenization solves the basic requirement to protect PII from hackers; the configurability has been harnessed to develop a new one-click solution to the RTBF problem. (That same configurability can also be harnessed to solve the other user rights issues.)

Rixon's RTBF solution is conceptually, if not technically, simple. Consider a traditional online purchase. The user accesses the online store (which is the Rixon customer), chooses a product, and enters transaction and payment details into a web payment form as usual. This PII goes straight to the tokenization engine, where it is tokenized. The store owner only holds the tokens, never the raw data.

The data is de-tokenized automatically for use when legitimately required by the store owner and allowed by the user – for example, to settle the transaction with the user's bank, or when viewed by the user in the original browser. However, the browser web form includes an additional button as well as the standard data Submit button. The second button is an Allow or Forget toggle.

The tokenized PII is tied to this form and this user – the data owner. When the Allow/Forget toggle is set to Allow, the store owner is allowed to detokenize the PII. But the moment the user switches the toggle to Forget, that permission is almost instantaneously withdrawn. The store owner can only see the meaningless tokens; and this is wherever and by whomever the data is used. To all intents and purposes – and certainly within the meaning of the legislation – the user's PII has been forgotten, and the law satisfied.

But Rixon's RTBF solution goes one step further. The tokens themselves have not been deleted, just rendered meaningless. The user still retains the Allow/Forget toggle switch. If this user wishes to make a second purchase in a few weeks' time, he or she can simply set the toggle to Allow, and the earlier tokens again become usable data without having to be re-entered. This PII can be forgotten and re-allowed as often as necessary.

In brief

Rixon Technologies solves the entire data protection and RTBF problem by removing it. Data protection is satisfied by ensuring the business only has tokens and no actual PII. If the customer is breached, there is no PII to steal. If the customer is audited, there is no PII to audit. And above all, responsibility for and authority over the Right to be Forgotten is removed to the user (data owner) through unique configuration settings determined by the service provider, based on the service provider's risk tolerance. Once the service provider passes control to the data owner, the service provider cannot reverse the decision by the data owner, but must wait until the data owner gives control back. Consent to use PII can be withdrawn by the user instantly at the flick of a switch – requiring no action from the company involved.

Rixon Technology's secure, configurable tokenization solves the business need to keep data protected while simultaneously handling the new range of user rights over that data.

RIXON
TECHNOLOGY

Visit us at **rixontechnology.com** to learn more.

✉ info@RixonTechnology.com / sales@RixonTechnology.com
☎ 972-377-0049