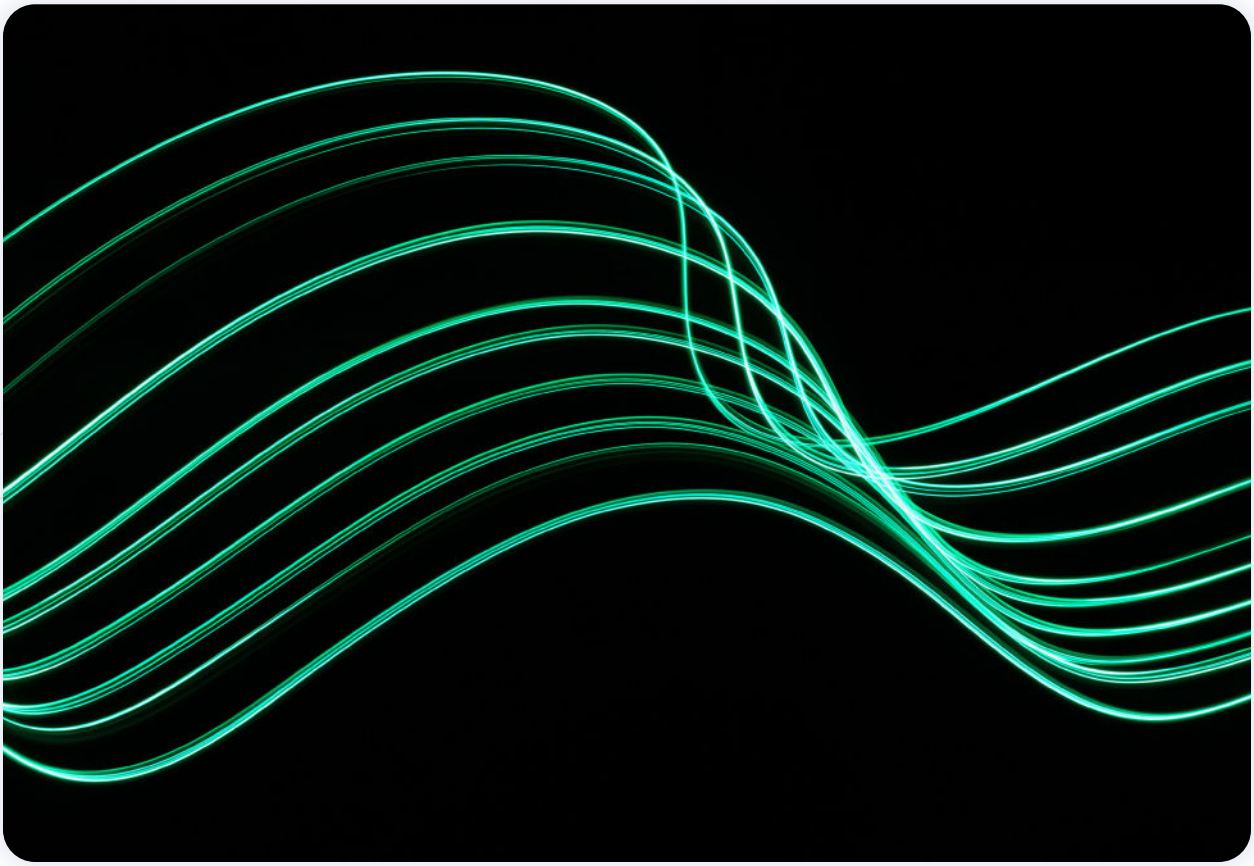


tokenex

GDPR Compliance Guide

How cloud tokenization can de-identify data to meet the requirements of GDPR and simplify the compliance process

Protecting personal data

As technology evolves and its presence in our lives continues to expand, our real-world identities become more and more intertwined with our digital footprints. This continued merging of the digital and the real has forever changed the privacy landscape.

To combat concerns surrounding the protection of our sensitive personal data, legislative and regulatory bodies have begun to establish laws and requirements for the handling of personal information. One of the first and most influential of these regulations is the European Union's General Data Protection Regulation (GDPR), which was passed in May of 2018.

To meet these obligations, we suggest leveraging a cloud tokenization solution to pseudonymize data at the point of acceptance, allowing it to pass through your internal systems in a secure, de-identified form. This can enable your organization to virtually eliminate the risk of data theft while preserving the business utility of the data you process.

Tokenization for de-identification

Pseudonymize data for security and utility

Universal token storage consolidates digital ecosystem

Simplify compliance via unified framework

Diverse token schemes for any structured data type

Strategies for compliance

Many methods exist for helping your organization comply with the GDPR, so finding the right one for your unique needs can be a challenge. In general, though, it is advisable to procure a solution that reduces the risk, cost, and effort required to satisfy the requirements of GDPR. In turn, you will simplify the compliance process and mitigate the difficulty of meeting your regulatory obligations.

Before you begin the compliance process, we recommend working with your in-house counsel, a certified data protection officer, or another legal and compliance expert. These individuals can guide you as you navigate the requirements of the regulations and assist in the decision-making process to ensure you're meeting your obligations under GDPR. The steps outlined below are intended to provide general guidance, not a prescriptive or exhaustive method for GDPR compliance.

Find and document all of the personal data in your internal systems

Known as data discovery, this process will enable you to determine the extent of personal data you possess and are therefore responsible for protecting. Using tools for data discovery and classification, you can streamline this process and help map the personal data in your environment. Once this data is discovered and documented, it is advisable to store it in as few areas as possible and to delete any data that does not provide immediate technical utility or business value.

Need a full list of key terms and concepts for GDPR?

Terms & Concepts

Determine what processes, and technology interact with that data

After you've mapped all of your personal data, you can begin to identify items that could potentially affect the security of that data. For instance, if you share personal data with a third party or if multiple employees have access to the area of your network where that data is stored, you should ensure those third parties or employees are operating in compliance with GDPR. Ideally, you would minimize the number of individuals and systems that come in contact with personal data to reduce the risk of that data becoming compromised or being handled improperly.

Create a consumer agreement for collecting, sharing, and storing personal data

This step should involve significant input from a legal and compliance expert. You will need to detail the types of data you're collecting, what they will be used for, and why they are being collected in the first place. Be sure to write an agreement that is clear and easy for consumers to understand. You will then need to present this agreement to data subjects to receive their consent before processing their personal data.

Continually evaluate your environment to maintain compliance

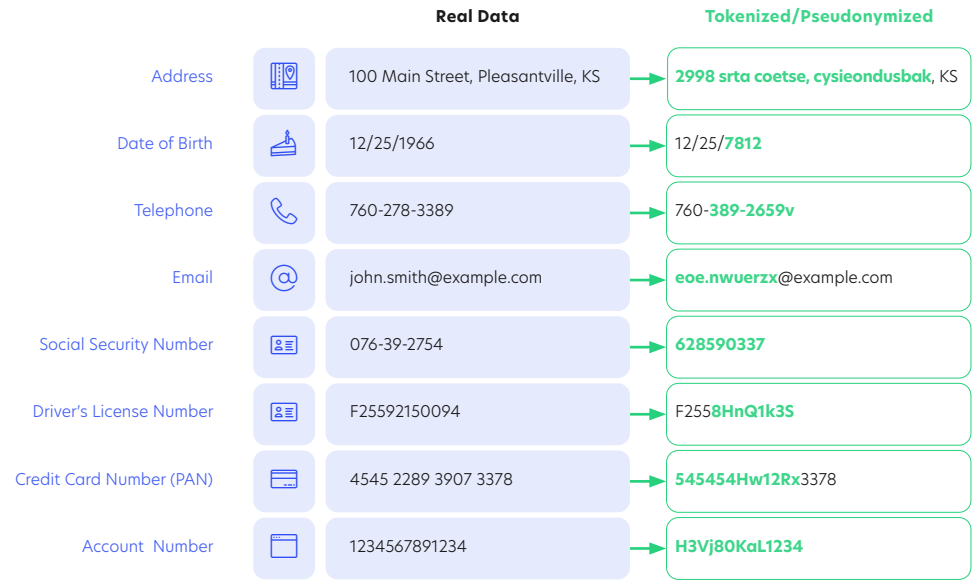
Regulatory compliance is not a one-time, "set it and forget it" obligation. It requires continuous review and maintenance to ensure your practices remain compliant. To do this, you should keep track of updates to the regulation and any changes to your network or methods for sharing or collecting personal data. Document these changes and address any instances of noncompliance accordingly.

Implement a security technology to pseudonymize data

Most companies do not have the resources necessary for maintaining constant global protection, detection, and incident response for the sensitive data they process. This is where security providers can fill the gap in an organization's defenses. When implemented properly, security technologies can play a significant role in helping to meet the requirements of GDPR.

How tokenization can help

With the right security controls in place, tokenization can protect sensitive data by removing it from your organization's environment and replacing it with a nonsensitive placeholder. This placeholder, known as a token, can retain certain aspects of the original data for business and analytics purposes without fully identifying itself. As a result, in the event that a breach occurs or the token is otherwise compromised or exposed, it will not be considered personal data because it will be without its identifying elements.



Additionally, tokenized data can be temporarily returned to its original form when the information is required for processing or is requested by the data subject. In the event that an individual requests to be forgotten, an organization can simply delete the token on the tokenization provider's system to comply with that request.

Yet another benefit of tokenization is that in the event of a data breach, an organization might not have to notify the affected individuals. If your environment becomes compromised, tokens—not personal data—are the only information that could be stolen. In effect, no data breach has actually occurred; therefore, there's no need to issue a breach notification.

Cloud security for GDPR compliance

Since its 2018 enactment, the GDPR has proven itself to be the world's most influential piece of privacy legislation. As more regulations follow suit, it is imperative to prepare your organization for the future of data privacy. Cloud tokenization can be a powerful tool for protecting data and positioning your organization for compliance. To learn more about GDPR, the TokenEx Data Protection Platform, or how TokenEx can help your organization protect its most sensitive data to reduce risk, minimize scope, and simplify compliance, contact us today at **info@tokenex.com**.

Your compliance journey starts right here.

Connect with us

Key terms and concepts

Personal data - Personal data is often used broadly to refer to all types of sensitive data, but within the context of the GDPR, it's defined as any data—name, email address, banking information, medical information, IP address, etc.—"related to an identified or identifiable natural person." The natural person portion is particularly important as it is used as the qualifier for another key term, data subject. In order for data to be considered personal data—and as a result, protected by the GDPR—it needs to be associated with a data subject.

Data subject - The full definition of a data subject according to Article 4.1 of the GDPR is "an identifiable natural person ... who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person...." Simply put, data subjects are individuals who can be associated with and identified by personal information.

Data processor - A data processor is any organization or entity that handles the personal data collected by the data controller. Although the controller is responsible for managing consent and other communications with data subjects, processors still can be penalized for noncompliance. They also face additional requirements specific to their roles as processors of the original data.

Consent - The consent of data subjects for processing their data is not required in every case, but it is strongly encouraged if an organization might not otherwise have a compelling or legitimate legal reason for retaining that data. When providing an agreement for consent, organizations are no longer allowed to use complicated, obscure, or other difficult-to-understand terms and conditions to gain consent for data processing. In other words, the individual granting consent must be able to clearly understand the terms of the agreement and must be given an opportunity to either refuse or accept.

Penalties - An organization found to be willfully or intentionally in violation of the GDPR is subject to administrative penalties of 4 percent of annual turnover or €20 million, whichever is greater. Accidental infractions or negligence of the data protection mechanisms in the GDPR can result in penalties of 2 percent of annual turnover or €10 million, whichever is greater. However, these fines do not include the cost of litigation, customer loss, systems changes, and other related fallout for failing to protect sensitive data.

Pseudonymization - According to Article 4(5) of the GDPR, pseudonymization is defined as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." The GDPR specifically mentions pseudonymization as an appropriate method for de-identifying data. In fact, Recital 29 mentions incentives for organizations to apply pseudonymization, and Articles 25 and 32 specifically call out pseudonymization as an appropriate technical measure for protecting personal data.

Breach notification policy - Organizations are required to report a data breach to a supervisory authority within 72 hours of becoming aware of the breach. If the breach is likely to put the rights and freedoms of the affected individuals at risk, those individuals must also be informed without undue delay. As part of any breach notification process, business continuity and disaster recovery are the top priorities. Security providers are especially helpful when responding to and recovering from a data breach. For example, if the personal data compromised in a breach has been de-identified using tokenization or a similar technology, an organization may not be obligated to notify the associated individuals.

Right to access & right to be forgotten - Individuals have the right to obtain confirmation from the data controller as to whether their personal data is being processed, where it is being processed, and for what purpose(s) it is being processed. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. Data subjects also can request that the controller erase and cease further dissemination of his or her personal data. This is also known as the right to erasure.

Privacy/data protection by design and default - Article 25 of the GDPR obligates organizations to institute data protection principles by design and by default. This concept requires data security to be built into the design of systems, as opposed to tacked onto existing processes and infrastructure. It also means that controllers are to hold and process only the data necessary to fulfill whatever need the data was collected for in the first place and to limit the access to customer data to the proper personnel. This practice is known as data minimization.

Return