GDPR AND THE FUTURE OF PRIVACY

CREATING A COMPLEMENTARY SOLUTION WITH TOKENIZATION AND SECaaS

ARMOR

TOKENEX
NO DATA. NO THEFT.

GDPR AND THE FUTURE OF PRIVACY

CREATING A COMPLEMENTARY SOLUTION WITH TOKENIZATION AND SECaaS

In 2018, the information security industry received a new standard for privacy: the European Union's General Data Protection Regulation (GDPR). Since its implementation on May 25, the law has revolutionized the way companies around the globe handle and store personal data, forcing entities to re-evaluate their methods for securing sensitive information and pushing security, IT and compliance professionals to find innovative solutions.

The goal of the GDPR is to standardize data privacy laws across the EU member states and to "protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy." As a result, how the personal data of EU citizens is managed will be held to a much higher standard, setting a precedent for privacy regulations worldwide.

The goal of the GDPR is to standardize data privacy laws across the EU member states and to **"protect and empower all EU citizens data privacy** and to reshape the way organizations across the region approach data privacy."

GDPR BASICS

PERSONAL DATA
The new definition

Under the DPD

- name
- photo
- email address
- phone number
- mailing address
- identifying numbers (bank acc. etc.)

Under the GDPR

- name
- photo
- email address
- phone number
- mailing address
- identifying numbers (bank acc. etc.)
- ✓ IP addresses
- ✓ biometric data (fingerprints, retina scans)
- ✓ mobile device identifiers
- ✓ geo-location
- ✓ behavioral & demographic profiling data

In January of 2016, the EU parliament agreed upon and adopted the GDPR as its new data privacy standard, replacing the Data Privacy Directive (DPD). The GDPR's key principles hold true to the DPD's, but they include changes aimed at protecting the personal data of natural persons (i.e., data subjects) from security breaches in today's ever-evolving threat landscape. Companies collecting and storing a data subject's personal data were provided a two-year grace period to ensure their policies and processes adhered to the GDPR's standards prior to its enforcement date.

In short, the GDPR expanded the definition of personal data, applied stricter laws to businesses processing that data and also empowered individuals with greater control over their data and how it's being used. A few key aspects of the GDPR include:

GEOGRAPHICAL SCOPE

Perhaps the biggest change for businesses between the DPD and the GDPR is its global reach. Any organization - regardless of geographical location – processing or storing the personal identifiable information (PII) of EU citizens must adhere to the GDPR's standards. This ensures that the data of natural persons is protected around the globe.

PENALTIES

Noncompliant businesses are faced with a substantial fine of up to 4 percent of the company's annual turnover or €20 million – whichever is greater.

CONSENT

Organizations are not permitted to use opaque terms and conditions to gain consent for data processing. Individuals must be able to clearly understand and agree to granting consent.

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 result in high risk to the rights and freedoms of the affected individuals, the individuals must also be informed without undue delay.

RIGHT TO ACCESS AND RIGHT TO BE FORGOTTEN

Individuals have the right to obtain confirmation from the data controller if their personal data is being processed, including where and for what purpose it is being processed. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. Additionally, data subjects 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 BY DESIGN

This concept requires data security be built into the design of systems, as opposed to tacked on later. It also means that controllers are to hold and process only the necessary data, limiting access to customer data to only the proper personnel.

The GDPR expanded the definition of personal data, applied stricter laws to businesses processing that data **and also empowered individuals with greater control over their data** and how it's being used.

THE RIPPLE EFFECT

In the nearly two years leading up to the GDPR's implementation, many thought it would bring an immediate barrage of fines sizable enough to almost shutter noncompliant companies. Thankfully, however, that has not been the case. Although we've seen a few penalties handed down, it takes time for regulators to properly conduct audits and conclude their findings.

One of the most interesting implications of GDPR is the number of other countries around the globe that are following suit. Brazil, India, Canada and the United States are already implementing data privacy laws similar to the GDPR, such as California's Consumer Privacy Act of 2018.

In India, a draft of the Personal Data Protection Bill 2018, inspired by the GDPR, has been submitted for consideration to the Indian government. Similarly, the Brazilian General Data Protection Law was signed into effect on Aug. 14, 2018. Its contents are also similar to GDPR's, and it is set to take effect in February 2020.

Additionally, Canada updated its data protection rules earlier this year to align with the GDPR. Albeit, Canada's regulations are not as stringent as the EU's – not yet anyway. For example, although the GDPR states that companies must notify regulators and consumers within 72 hours of any data breach, Canada's new federal data breach requires companies to disclose only a security breach that "post(s) a real risk of significant harm" to the federal privacy commissioner and consumers, "as soon as feasible." However, despite more lenient rules at this point, Canadian officials and regulators want to go beyond GDPR. In fact, the former information and privacy commissioner for the Canadian province of Ontario, Dr. Ann Cavoukian, said, "It would be almost like a step back for us not to raise the bar."

Prior to the GDPR's rollout, U.S.-based companies not collecting or storing personally identifiable data from EU citizens debated whether the regulation applied to them. Although these companies technically aren't subject to the GDPR, a similar law likely will apply to them in the near future. Compliance experts are encouraging the use of the GDPR as a baseline privacy framework, regardless of where an organization is located and from where it is collecting data. Because so many countries plan to implement privacy regulations soon, it is prudent for companies to prepare accordingly.

Compliance experts are encouraging the use of the GDPR as a baseline privacy framework, regardless of where an organization is located and from where it is collecting data. Because so many countries plan to implement privacy regulations soon, **it is prudent for companies to prepare accordingly.**

GDPR COMPLIANCE AND SECURITY

As previously mentioned, the overall purpose of GDPR is to protect the data of natural persons in the EU from the onslaught of today's cybersecurity threats. Only meeting minimum compliance requirements is not sufficient. To truly secure customers' data, organizations need to develop strategic security programs. By doing this first – before even considering the laundry list of compliance regulations – companies will satisfy the majority of their GDPR responsibilities.

TOKENIZATION AND GDPR

SOLUTION

PARTIAL SOLUTION

GDPR ARTICLE	STATEMENT
Article 6 Lawfulness of processing 6(4)(e) – "the existence of appropriate safeguards, which may include encryption or pseudonymization.	If you are a data controller who has a valid reason--other than consent from the data subject--for the processing of his or her personal data "for a purpose other than that for which the personal data have been collected", Article 6(4)(e) obligates you to use "appropriate safeguards, which may include encryption or pseudonymization. The TokenEx platform enables you to pseudonymize personal data within your environment, by replacing it with tokens, and storing the personal data in an encrypted TokenEx cloud token vault.
Article 17 Right to erasure ('right to be forgotten') "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay…"	Article 17 allows a data subject to request a controller delete his or her personal data. Under Article 12(2), pseudonymization of data may provide some relief regarding Article 17 compliance. Article 12(2) states that, "The controller shall facilitate the exercise of data subject rights under Articles 15 to 22… unless the controller demonstrates that it is not in a position to identify the data subject." The TokenEx platform enables you to pseudonymize personal data stored within your environment by replacing it with tokens and storing the data in an encrypted TokenEx cloud token vault. This degree of pseudonymization and method of implementation may allow you to assert that you are not subsequently able to reliably identify the data subject, thus enabling the tokenized (pseudonymized) data to remain in use.
Article 15 Right of access by the data subject **Article 16** Right to rectification **Article 18** Right to restriction of processing **Article 20** Right to data portability **Article 21** Right to object	The remaining data subject access rights in the GDPR also allow a data subject to restrict or compel a controller to adjust processing in some way. Again, Article 12(2) may provide some relief from these obligations. Article 12(2) states that, "The controller shall facilitate the exercise of data subject rights under Articles 15 to 22… unless the controller demonstrates that it is not in a position to identify the data subject." The TokenEx platform enables you to pseudonymize personal data within your environment by replacing it with tokens. This degree of pseudonymization and method of implementation may allow you to assert that you are not subsequently able to reliably identify the data subject, to avoid having to return (right of access), correct (rectify inaccuracies), restrict processing, or transmit to another entity the tokenized data, yet to continue using it (object).

Article 25
Data protection by design and by default

"…the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles...."

The GDPR requires "data protection by design and by default." Article 25(1) specifically obligates controllers to "…implement appropriate technical and organizational measures, such as pseudonymization."

The TokenEx platform enables you to pseudonymize personal data within your environment, replacing it with tokens, and storing the data in an encrypted TokenEx cloud token vault. The pseudonymized data will likely present a lower risk, thus possibly reducing the number of additional security measures required to meet this obligation. Using a cloud-based tokenization provider like TokenEx to pseudonymize direct identifiers in the personal data your organization controls is a clear indication that you are considering data protection by design and striving to implement technical measures appropriate to the risk.

Article 32
Security of processing

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures…

Article 32(1) obligates controllers as well as processors to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk," including pseudonymization of personal data.

The TokenEx platform enables you to pseudonymize personal data within your environment, replacing it with tokens, and storing the data in an encrypted TokenEx cloud token vault. The pseudonymized data will likely present a lower risk, thus possibly reducing the number of additional security measures required to meet this obligation.

Armor security services allows for the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident, while employing a process of regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Article 33
Notification of a personal data breach to the supervisory authority

Article 34
Communication of a personal data breach to the data subject

The GDPR specifies new requirements for notification in the event of a breach of personal data. Under Article 33(1), a controller is required to notify supervisory authorities of a breach within 72 hours unless "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." Similarly, Article 34(1) stipulates that data subjects must be notified "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons…"

When evaluating the risk posed by the data breach, the level of pseudonymization of the data will certainly play a role. The TokenEx platform enables you to pseudonymize personal data within your environment, replacing it with tokens, and storing the data in an encrypted TokenEx cloud token vault. The pseudonymized data will likely present a lower risk, thus possibly reducing the number of additional security measures required to meet this obligation.

TOKENIZATION OVERVIEW

Tokenization is the process of replacing sensitive data with nonsensitive data known as tokens. It also can be used for the pseudonymization of data, making it an effective security and compliance measure that's especially valuable for meeting GDPR requirements and protecting sensitive data sets.

For example, instead of keeping an individual's identification number, date of birth and address behind on-premise security devices like firewalls, organizations can use tokenization to turn all that personal data into a token which can then be removed from your environment and securely vaulted in a tokenization provider's cloud.

With the right security controls in place, the information can be temporarily detokenized when it is required for processing or is requested by the data subject. If an individual requests to be forgotten, one can simply delete the token on the tokenization provider's system to comply with that request.

Another benefit of tokenization is that in the event of a data breach, an organization may not have to notify the affected individuals. If a threat actor infiltrates your environment, tokens – not PII – are the only pieces of information that could be exfiltrated. In effect, no data breach has actually occurred.

Although this scenario has been specific to protecting personal data, tokenization spans a variety of industries. In fact, TokenEx – a leading cloud-based tokenization solution – originally developed its groundbreaking platform for the purpose of securing payment card information. Additionally, tokenization is often used within the health care industry for deidentifying and sharing medical research across environments without compromising patient information.

TOKENIZATION AND SECURITY-AS-A-SERVICE

Organizations pursuing GDPR compliance are moving away from standalone tools and instead seeking flexibility, automation, orchestration and visibility in their cloud environments. Providers such as Armor and TokenEx offer these security conveniences. Tokenization also helps reduce the complexity of managing your security posture by eliminating the risk of sensitive data being stolen.

Companies collect different types and amounts of data daily, but they typically need to access an individual's personal information only a handful of times throughout the year. Storing sensitive information on premise, even with the strongest security posture, still poses a risk of a data breach. Partnering with tokenization and SECaaS providers is a way to mitigate those risks and focus on maintaining and building your business.

Instead of keeping an individual's identification number, date of birth and address behind on-premise security devices like firewalls, **organizations can use tokenization to turn all that personal data into a token** which can then be removed from your environment and securely vaulted in a tokenization provider's cloud.

SECaaS AND TOKENIZATION

TOKENEX
NO DATA. NO THEFT.

ARMOR

THE COMPLEMENTARY SOLUTION FOR THE PRIMARY TENANTS OF THE GDPR

Requirement	Solution
Geographical Scope Any organization processing or storing the PII of EU citizens must adhere to the GDPR.	SECaaS offers global protection, detection and incident response, and tokenization can diminish the risk of data theft during a breach.
Breach Notification Policy Organizations must report a data breach within 72 hours. Individuals must be informed without undue delay.	Data deidentified via tokenization may not require notification since the exposed data is no longer considered identifiable.
Right to Access and Right to be Forgotten Data subjects can request that the controller erase and cease further dissemination of personal data.	Tokenization enables organizations to delete tokens, destroying the information associated with the token and preventing the organization from ever detokenizing or restoring the tokenized data.
Privacy by Design Data security must be built into systems, as opposed to tacked on later. Controllers are to hold and process only necessary data, limiting customer-data access to the proper personnel	Using SECaaS and tokenization providers can demonstrate a company's efforts to comply. Data minimization can be achieved by keeping necessary data only for the time required to use it.

GEOGRAPHICAL SCOPE

With the GDPR's global scope, maintaining compliance and security everywhere is paramount. Most organizations do not have the resources for true 24/7/365 global protection, detection and incident response for the sensitive data they process. SECaaS providers can fill this gap in an organization's defenses, while tokenization can diminish the risk in the event of a breach.

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. Simple negligence of the data-protection mechanisms in the GDPR can result in penalties of the greater of 2 percent of annual turnover or €10 million.

By specifying financial penalties for GDPR noncompliance, the EU has essentially provided threat actors with a price list. Their ransomware ask is now a competitive "sale" against these GDPR penalties, which makes it increasingly important for companies to become compliant sooner rather than later. Organizations simply focused on appeasing EU data-protection authorities are overlooking the primary threat of a GDPR-related fine.

DATA SUBJECT RIGHTS INCLUDING CONSENT, RIGHT OF ACCESS AND RIGHT TO BE FORGOTTEN

Under the GDPR, organizations are required to provide clear and concise explanations of how they intend to use an individual's personal data so that he or she can provide informed consent. Organizations are also obligated to allow individuals to request access to their data and to know how it is being used. Lastly, individuals must be able to withdraw their consent for processing and request the organization delete his or her personal data.

Tokenization can help address the right to be forgotten in particular by enabling organizations to delete tokens. This destroys the information associated with the token and prevents the organization from ever detokenizing or restoring the tokenized data. Consequently, any place that token is stored in an organization's systems, including backup files and disaster-recovery sites, ceases to contain reidentifiable PII.

BREACH NOTIFICATION

As part of any breach-notification process, business continuity and disaster recovery are crucial. Meeting the GDPR's 72-hour notification requirement is only the beginning. Responding to and recovering from a data breach is where SECaaS can deliver, and if the personal data compromised in a breach has been deidentified using tokenization, an organization may not be obligated to notify the associated individuals since their exposed data is no longer considered identifiable information.

DATA PROTECTION BY DESIGN

Article 25 of the GDPR requires organizations to consider data protection by design and by default. Using a SECaaS and a tokenization provider are both ways in which a company can demonstrate its efforts to comply with this article. Data minimization is also an important component of a data-protection strategy. To meet both security and compliance standards when handling PII, every company's goal should be keeping necessary data only for the time required.

Tokenization can help address the right to be forgotten in particular by **enabling organizations to delete tokens.** This destroys the information associated with the token and prevents the organization from ever detokenizing or restoring the tokenized data.

A Complementary Solution

Today's threats are real, and stringent compliance obligations, such as the GDPR and the Payment Card Industry Data Security Standard, penalize companies for not protecting themselves. By combining tokenization and SECaaS for a complete security solution, customers of Armor and TokenEx can safely meet multiple compliance obligations and keep up with the ever-shifting cybersecurity and regulatory landscapes.

Since 2014, Armor has been securing TokenEx's private cloud. This partnership joins two leading data-protection companies, providing improved performance along with unsurpassed security for TokenEx's cloud-tokenization, encryption, data-vaulting and key-management solutions.

ARMOR®

TOKENEX
NO DATA. NO THEFT.

To learn more about tokenization and how TokenEx can help you to secure any sensitive data set and achieve compliance, contact us at www.tokenex.com or email us directly at: **info@tokenex.com.**