Executive Brief

New European Rules Hits Companies Everywhere

Secure and Protect Your Customer's Private Data During Transmission and Storage

July 7, 2018

This report provides an executive overview of new European privacy and data security regulations with an emphasis on safeguarding data during its transmission and while in storage on a server. If your company holds and processes personal information, the General Data Protection Regulation (GDPR) more than likely applies and compliance is necessary.

Effective May 25, 2018 companies doing business in the European Union (EU) are required to comply with the GDPR, even if the company is based elsewhere. GDPR applies when transferring personal data outside of Europe, including customers, employees and business contacts such as suppliers. s

The GDPR has a very long reach, requiring organizations located inside AND outside of the European Union to adhere to the rules. The obligations imposed on businesses cover the processing of personal data of individuals, broadly defined as "any information relating to an identified or identifiable natural person". This includes:

- Any operation or set of operations which is performed on personal data or on sets of personal data.
- The definitions are broad and encompass a range of data types and a variety of data usages such as log-in information, IP addresses, vehicle identification numbers. physical address, email, address, cookie ID information, Internet Protocol (IP) address, and even the information your business collects in its customer relationship management (CRM) system.
- Even though this information may not enable direct identification of individuals, if it indirectly identifies individuals, it is considered personal data under GDPR.

KEY POINTS

- GDPR has a global reach
- High non-compliance penalties
- Customer data must be secure
- There are 3 key obligations for data storage and transmission
- Cybercrime is a growing threat
- MicroEncryption® is the most secure method to prevent the breach of customer data

In practice, this means that most services and/or projects will be considered to involve processing of personal information, including the transmission and storage of digital data.

There are many areas of the GDPR for companies to implement including policies and processes to comply, placing a burden on businesses of all sizes. However, a portion of the GDPR that companies can and should quickly implement revolves around the protection of private information during the transmission and storage of personal information to ensure adequate data security. Doing so will demonstrate GDPR compliance – and prevent a beach by cybercriminals.

The three key responsibilities and principles that companies must comply with under the GDPR concerning transmission and storage of personal data are:

1. All Personal Identifiable Information (PII) must be protected. Customers (and regulators) are demanding that their valuable digital assets are safe and not compromised by cyber criminals.

2. The new rules are pushing firms to pseudonymize PII prior to processing it, meaning that the data can't be attributed back to a particular person. In this context, pseudonymize refers to a data management procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.
3. Companies must store user personal data and information about their actions separately. For example, a name is stored separately from the history of this person's actions. In this case, a data leak won't allow the cybercriminal to find out to whom these actions belong.

The GDPR calls for large penalties when companies fail to comply with these new obligations. Any business located anywhere in the world that has at least one customer in the European Economic Area must comply. Otherwise they risk penalties as high as €20 million (more than $24 million) or 4% of a company's total global revenue, whichever is larger.

Most companies affected by the GDPR are NOT ready to comply fully with its requirements. In the United Kingdom the government released the results of a survey showing that as few as 38 percent of companies in the UK have heard of GDPR[1]. It is likely that far fewer businesses are aware of GDPR in other areas of the world.

Aside from the requirements to protect customer information during its transmission and while in storage on a server, the focus of this report, there are many other aspects to GDPR compliance. For the full detail on the rules for the protection of personal data inside and outside the EU, please visit the official website of the European Commission[2].

Must Have Cybersecurity Platform Characteristics to Comply with GDPR

Besides potential financial penalties, cybercriminal related data breaches risks include:

- Loss of critical data and revenue due to business interruption and system downtime.
- Customer flight because of lack of trust and bad publicity.
- Legal actions by customers and regulatory agencies.
- And the in the worst-case scenario – business shutdown.

While organizations should be concerned about the potential significant financial penalties, forward-thinking companies are using GDPR as the impetus to make their privacy and data security policies an asset as well as a competitive advantage to meet the growing concern and demand for secure private data.

[1] https://www.zdnet.com/google-amp/article/gdpr-deadline-looms-but-businesses-still-arent-ready/

[2] https://ec.europa.eu/info/law/law-topic/data-protection_en

Simply put, customers will only want to do business with companies they trust with their data and who stand up for protecting their valuable digital assets from being compromised by cyber criminals and cyber-spies.

A comprehensive approach is required with a strong emphasis on storing and accessing the most private digital information people have. Threats are constantly evolving and the best defense needs to offer the most robust protection against the newest wave of cyber attacks.

Based on the above three key responsibilities and principles of GDPR, the following is your guide to the attributes needed to create a solid shield against cyber intrusion to protect your customer's most valuable assets – their private data:

1. The starting point to selecting a cybersecurity method to safeguard your customer's data is to accept that a determined hacker will get through your perimeter defenses, sooner or later. Recognizing this, the goal then is to encode the data in such a way that it is extremely difficult, if not impossible, for cybercriminals to get to your most sensitive data and obtain any useful information.
2. There are four techniques to consider to accomplish this – Blockchain, public-key infrastructure (PKI), encryption techniques, and MicroEncryption®.

   Blockchain: Blockchain has the potential to transform our world, yet it is a relatively new technology and isn't nearly as secure as other "battle tested" methods. In its current state of maturity, blockchain is not a security architecture and has significant weaknesses and limitations. Plus, blockchain is slow, causing issues for identity management applications when resolution often needs to be immediate – not to mention large files such as videos and medical imaging – affecting the user's experience.

   Public-key Infrastructure: Many companies are using PKI because it's the standard of the Internet and considered to be secure – if implemented correctly, which it rarely is. PKI is subject to compromise even when setup properly as hackers and their computers are getting better at solving cyber puzzles. Once the holder of the public key is breached, bad actors have access to the entire system. Also, like blockchain PKI is relatively slow, adding delays for large media files such as video transfer. As past cyber intrusions have shown, PKI is becoming less effective as a defense against corporate intruders.

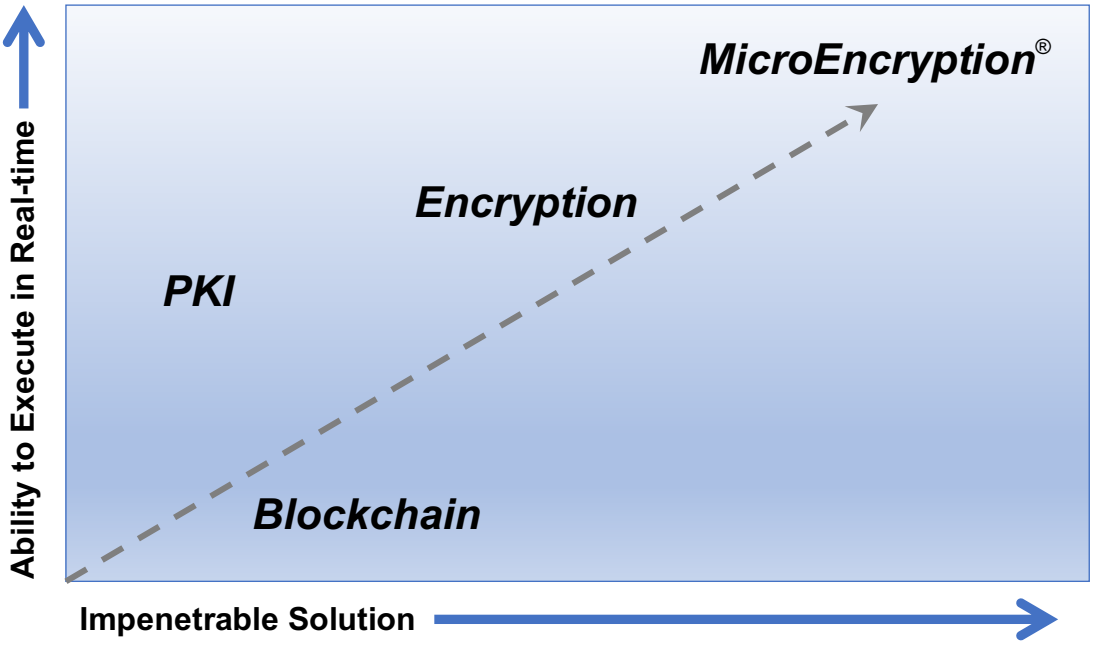
   Encryption: There are several encryption standards available such as the Advanced Encryption Standard (AES) and all offer challenges to keeping information safe. Encryption encodes the entire data structure as a block, including the framing bits, embedded addressing bits, and start/stop bits. Because of this, the entire data stream to is open to hacking. In fact, breaches are common that extract thousands, if not millions of customer records at the same time. Plus, encryption reduces application speeds and can impact the user experience.

   MicroEncryption: Tokenization has been utilized for many years and has yet to be broken. MicroEncryption is based on proprietary tokenization technology originally created to prevent the theft of credit card numbers while being stored. Unlike the bulk technique of

encryption, MicroEncryption replaces sensitive customer data, at the byte level, with MicroTokens™ that are useless to hackers.

A MicroToken is similar to a credit card type of token, yet stronger because it doesn't use any piece of the original data to create it. Each individualized portion of data is replaced and removed from its stored location, and then individually encrypted. When a breach occurs, hackers cannot access the sensitive data because it is no longer there – only useless place holders, or MicroTokens, exist that do not allow access or knowledge of where the "real" data in located. In addition, each individual piece of data that has been relocated is encrypted with custom or standard algorithms, typically AES 256, is then broken up into smaller pieces that are randomly disbursed among multiple disk drives throughout different locations.

Another MicroEncryption advantage is its processes add very low latency of transmission and access, allowing for real-time applications usage that do not affect the user experience.



3. Protecting customer's data with pseudonyms offers one of the best defenses against cyber breaches as the actual data is no longer maintained in a location that cyber thieves can access, as they do not even know the new location exists.

   MicroEncryption substitutes MicroTokens for real data, which are placeholders, that do not contain any part or piece of the original sensitive data elements. If a breach were to occur there isn't any sensitive data within that system to be exploited because it is no longer there. It has been removed and is now represented by a MicroToken.

Variations of MicroTokenization algorithms add meaningless chafe into the transmission while the data is transmitted, known as data-in-motion. This all adds up to the most reliable and highest protection level possible.

4. For data-at-rest, storing personal data in a separate and hidden location is a very strong method of protecting sensitive and private information. With MicroEncryption each data element is secured and protected as if it were its own database with its own sets of keys while being stored. This is impossible to do with bulk encryption.

   When MicroEncryption is applied to a database, MicroTokens are substituted for the original data elements. Then each individual data field is encrypted, secured, and randomly scattered across various hard drives in different locations.

   Because every piece of data is secured individually down to field level, if somehow a hacker was able to breakthrough your defenses a mass breach is eliminated.

   As an example, if you have a million social security numbers stored in your database, you're MicroEncrypting a million times. On top of that that, each social security number can be encrypted again into nine additional induvial encoded pieces. It is virtually impossible to de-encrypt nine million times within milliseconds with today's existing computing power.

   If a breach were to occur, no sensitive data within the system could be exploited.

Protecting your customer's data with the strongest mechanism possible offers the best defense against cyber breaches and thus the best protection. The strongest shield you can put in place is a cybersecurity platform based on MicroEncryption.

This is also a good way to show both your customers and EU regulators that that your company is serious about privacy.

Earn and Maintain Your Customer's Trust

Companies must have sufficient security to avoid data from being compromised, including technical security, training, and robust processes and procedures. Now is the time to implement additional controls and make data security a strategic asset to your business.

MicroEncryption exceeds industry security standards and regulations by securing one piece of data at a time in real time. Even if hackers pierce the firewall and perimeter defenses, they will only find meaningless MicroTokens.

MicroEncryption is scalable and designed to evolve with future best practices of the security world, without sacrificing either cybersecurity or accessibility. It is an advanced solution relevant across all industries including banking and financial services, healthcare, insurance, cloud application services, manufacturing, transportation, energy and utility, retail, supply chain management, and defense and government sectors.

About Eclypses™

Eclypses' industry leading disruptive cybersecurity software replaces user data with MicroTokens™ using MicroEncryption® to provide the highest level of data privacy available. With the company's patent pending MicroToken Exchange™ (MTE) technology, real data is never exposed when transmitted or while stored on servers and remote devices.

Applications range from secure command and control needs, including Internet of Things (IoT), to secure storage and retrieval of sensitive data, such as credit card information and healthcare records. Eclypses' MicroToken Exchange technology is helping enterprises and government agencies protect their most sensitive and private information from cybercriminals cyber terrorists today.

Eclypses' MicroToken Exchange™ (MTE) software complies with the European Union's General Data Protection Regulation (GDPR). In addition, Eclypses' technology is certified as Payment Card Industry Data Security Standard Level 1 (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA) compliant.

The Digital Safety Deposit Box of CertainSafe®, a business unit of Eclypses, has been selected as a 2018 Editors' Choice Product by PC Magazine (PCMag) for best encryption software. In addition, the Digital Safety Deposit Box was designated as the most secure solution tested. The Digital Safety Deposit Box is an ultra-secure cloud-based service that makes it easy for businesses to securely store, access, and share valuable and private assets, and is built on Eclypses' cybersecurity software.

In recapping the coveted award, PCMag's Lead Analyst for Security Neil J. Rubenking writes, "When backing up your sensitive files to the cloud, CertainSafe Digital Safety Deposit Box emphasizes security over all else, but it doesn't sacrifice ease of use." Rubenking added that of all the solutions reviewed, "The Digital Safety Deposit Box has the most secure encryption software."

Located in Colorado Springs, Colorado, you can contact Eclypses at 719-323-6680 or via email at info@eclypses.com. Please visit us at www.eclypses.com and www.certainsafe.com.