FUTUREX

WHITEPAPER

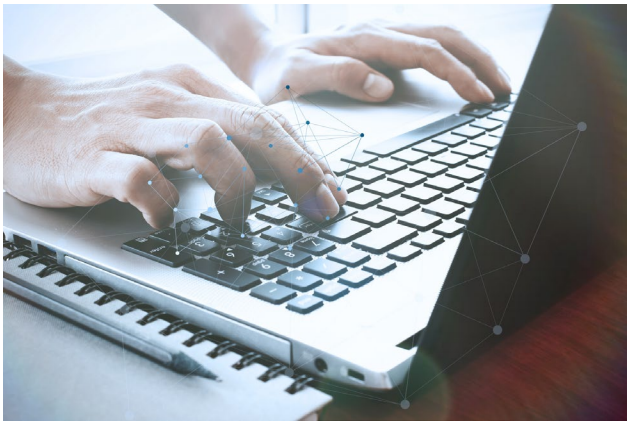
Data Privacy Legislation: Infosec Implications

LGPD, GDPR, and Other Emerging Regulations

DATA PRIVACY LAWS

As cyber-attacks and data security breaches become more frequent in today's digital landscape, multiple countries are seeking to install more stringent regulations for organizations that handle sensitive customer data. This legislation affects all organizations that collect any form of sensitive data including names, addresses, browsing histories, and anything else that could potentially be used to identify or discriminate against a customer. This whitepaper will provide a high-level overview of the common standards to which each new legislation will hold organizations conducting business in their region, as well as what steps organizations can take to become compliant.

COMMON ELEMENTS OF THE REGULATIONS



Currently, there are over 120 countries world-wide considered to have taken meaningful steps towards establishing security standards for data protection and customer privacy.[1] Some of the most well-known recent legislation changes contributing to this security movement are the EU's General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD), both of which apply to any business done in the region and will be compared and explored further in this whitepaper.

GDPR and LGPD, amongst other data security regulations, cover similar elements, with a split focus between data privacy and data protection. In terms of data privacy, both documents place an emphasis on customer consent and involvement. For example, both the GDPR and the LGPD created rules for the expansion of basic rights for data subjects, including granting subjects the ability to request that their data be removed from any database and mandating that organizations collecting data must allow subjects to "opt-in" to collection, and must clearly communicate with subjects when a data breach occurs.

The general legislation in both sets concerning data protection and security is considerably more vague. Each set of legislation specified new data security responsibilities for organizations and the consequences for breaching such responsibilities (mainly large fines up to 4% of global revenue,) but are less detailed when it comes to how exactly to fulfill them. For example, the LGPD outlines a "principle of accountability" for organizations, stating that "both data controller and data processor should take appropriate technical, security, and administrative measures to protect personal data. The data protection authority may provide for minimum technical standards, considering the nature of the data handled, the specific characteristics of the treatment, and the current state of technology."[2] Similarly, the GDPR states that organizations must follow the principle of "privacy by design", which states that organizations "shall implement appropriate technical and organizational measures… in an effective way… in order to meet the requirements of this Regulation and protect the rights of data subjects."[3]

---

[1] Leite Monteiro, Renato, "The new Brazilian General Data Protection Law." https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/
[2] Leite Monteiro, Renato.
[3] EU GDPR.org, "GDPR Key Changes". https://eugdpr.org/the-regulation/

LGPD AND GDPR SOLUTION OVERVIEW

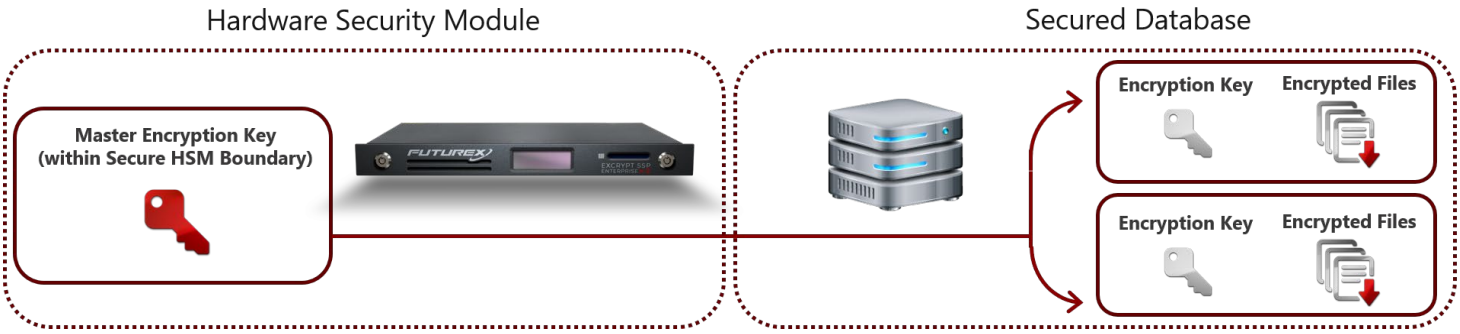
In short, it is the responsibility of the organization collecting and controlling customer data to ensure that they have done their due diligence to implement a comprehensive data security infrastructure into every part of their organizational processes. Additionally, if organizations can show their due diligence, they do not have to notify customers of security breaches. How such a security infrastructure is to be achieved, however, is left open ended. For many organizations that are subject to GDPR, this is where hardware security modules (HSMs) and data encryption came in to play, and where organizations under LGPD will likely need to turn in the coming months.

GDPR	LGPD
Organizations doing business in the EU	Organizations doing business in Brazil
Released April 14th, 2016	Released August 14th, 2018
Came into effect May 25th, 2018	Came into effect February 1st, 2020

HOW TO ENSURE COMPLIANCE

The best way to ensure that organizations that handle sensitive data are in compliance with new legislation is to integrate strong cryptography and key management backed by HSMs into their existing data infrastructure via database platforms. HSMs are dedicated, standards-compliant cryptographic appliances designed to protect sensitive data in transit, in use, and at rest using physical security measures, logical security controls, and strong encryption.

Encryption is made possible using encryption keys—randomly generated values that must be kept secret in order to protect the encrypted keys. HSMs generate and store the keys used for encrypted communication among devices within a Secure Cryptographic Device (SCD) to ensure a level of security that software alone cannot supply. When information is sent to the HSM via a trusted connection, the HSM allows for the quick and safe encryption or decryption of that information using the appropriate key.



Organizations may integrate their existing database platform with an HSM to increase security and meet regulatory compliance requirements. This integration is done using a cryptographic application to communicate between the database platform and the HSM.

There is currently no specifically legislation-compliant application for the integration of database platforms with HSMs. However, because most current database platforms are compliant with strong, FIPS-validated cryptographic libraries such as PKCS #11 and KMIP, it is not difficult for organizations to achieve compliance by integrating with and offloading their cryptographic and key management processes to an HSM. Optionally, organizations may also choose to develop their own applications for HSM integration.

NEXT STEPS FOR ORGANIZATIONS

For organizations seeking to ensure their compliance to new legislation, it is in their best interest to perform an audit of their current organizational infrastructure, locate the database platform(s) in which they store sensitive data, and use a cryptographic library to integrate each platform with an HSM. Organizations should seek a trusted provider of hardware security solutions to fulfill their cryptographic needs.

By following these steps, organizations will be capable of demonstrating their due diligence towards comprehensive data security and compliance with new regulations with minimal to no disruption of their current infrastructure and day-to-day processes. To learn more about GDPR, visit the EU GDPR website. To find more information about LGPD, read an English overview and download the Portuguese document here.

For any questions regarding regulatory compliance, hardware security modules, or application integration, reach out to a Futurex Solutions Architect or visit the Futurex website for more information.

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163