Brazil LGPD Protection of Critical Assets

Use case, Messaging and Prospecting Assets

Background & Context

The message is simple - robust Cybersecurity has become mandatory. If you're customer collects personal data and / or conducts business with or in the country of Brazil, they MUST comply with the Brazilian Lei Geral Proteção de Dados Regulation. On August 14, 2018, after eight years of debates and drafting, the Brazilian president sanctioned the Brazilian General Data Protection Law (LGPD). Therefore, given the 18 months of vacatio legis, the LGPD will become effective in February 2020.

This document is for IBM sellers and partners and meant to serve as a reference guide for how Data Security intersects with Brazilian General Data Protection Law (LGPD) code. In this guide you will find this section on background and context, a section on Use Cases and a sample Call Script and Social Selling guidance.

What is the LGPD regulation?

The law's key provisions closely mirror the European Union's General Data Privacy Regulation ("GDPR"), including significant extraterritorial application and vast fines of up to two percent of the company's previous year global revenue (the GDPR allows for up to four percent in certain aggravated circumstances).

What is the Scope of the new Law

The LGPD claims broad applicability, even outside of Brazil, in provisions that may be even more extensive than those in GDPR. It applies to any processing: (1) "carried out in the national territory" (i.e., in Brazil); (2) associated with the offering of goods or services in the national territory or involving the personal data of individuals located in the national territory; or (3) of personal data collected in the national territory. As under the GDPR, this broad scope applies to processing activities conducted wholly outside of Brazil, but which affect or target Brazilian citizens.

Lawful Bases for Processing. Similarly, the LGPD recognizes lawful bases for processing, including most notably, consent, contractual necessity, and necessity to fulfill the legitimate interests of the controller or a third party. As under most privacy frameworks, additional protections apply to certain categories of data, such as the personal data of minors and "sensitive data."

Unlike, the GDPR, however, the LGPD also lays out some additional, more specific bases, such as for the protection of health in a procedure carried out by health professionals and the protection of credit. The law also provides that the consent requirement will be considered waived where the data subject has "manifestly made public" his or her personal data.

Background & Context cont.

Although the law was passed in the Senate back in July, the version signed by the President included several small, but potentially meaningful, changes. The President had until August 14 to approve the bill, reject it, or make line item vetoes and sign a modified version of the bill. The President opted to veto three provisions: the establishment of an independent data protection authority, the ability to suspend or prohibit data processing for violations of the law (though judges may still impose such penalties through other existing laws), and the requirement that public actors disclose transfers among government agencies (though the law still requires that government officials communicate when they carry out processing, for what purpose, and via which procedures).

Data protection advocacy groups worry that these vetoed provisions may serve to gut the protections arduously labored over for months in the legislature, but the President's office suggests that these vetoes were the result of procedural defects and not an attempt to lessen the effectiveness of the law. For example, the President announced that his office would separately send a bill to Congress for the creation of a data protection authority.

Key takeaways:

- Brazil has enacted its Data Protection Law, the LGPD. Inspired by the EU's GDPR, the LGPD is the first law of its kind in Brazil and a landmark for the region. Brazilian data subjects will now have more control over their personal information, including the right to access, correct and delete it.
- Under the LGPD, companies processing personal data in Brazil will have to comply with a sweeping new set of obligations to disclose and limit the processing of data, keep the data secure and disclose if the data is breached. The LGPD also imposes requirements for transferring personal data out of Brazil, including that the receiving organization or country must provide a level of data protection comparable to the LGPD's.
- Companies have 18 months to conduct the diligence, gap analysis and remediation steps to get ready and avoid the LGPD's potentially severe financial penalties.

In passing this law, Brazil has significantly increased its data protection regime, and may be looking to prove its "adequacy" under the EU standard for data transfers. This would make Brazil one of the few countries to provide comparable data privacy protections as those offered to EU residents.

The law goes into effect 18 months after signing, giving companies until 2020 to bring their data processing practices into compliance.

Source: Inside Privacy - Updates on developments in data privacy and cybersecurity - FROM COVINGTON & BURLING LLP - By Melanie Ramey on August 20, 2018

Offering Alignment

Key Acts of the Brazilian General Data Protection Law (LGPD

There are 65 Articles over 10 Chapters, with each Chapter containing multiple Sections. This is a substantial bill. There are many Sections and Acts of the bill that are applicable to data security, these are some of the major ones. More details on these sections/Articles can be found in the Acknowledgements section of this. Each section contains a brief listing of the code in italic font and then comments on where Data Security fits with it.

Art. 9 – The data subject has the right to facilitated access to information concerning the processing of her/his data… - **GA, GVA, DRM**

Art. 12 – Anonymized data shall not be considered personal data, for purposes of this Law… - **GDEZ, MDE, GDE, SKLM**

Art. 13 – When carrying out public health studies, research entities may have access to personal databases – **GDPD, GDPF, GPBD, GPDI**

Art. 14 – The processing of personal data belonging to children and adolescents… **GA, GVA, DRM**

Art. 16 – Personal data shall be deleted following the termination of their Processing… - **GDEZ, MDE, GDE, SKLM**

Art. 18 – The personal data subject has the right to obtain the following from the controller… **GA, GVA, DRM**

Art. 19 – Confirmation of the existence of or access to personal data shall be provided by means of request by the data subject… - **GA, GVA, DRM**

Art. 22 – The defense of the interests and rights of data subjects may be carried out in court..- **DRM**

Art. 25 – Data shall be kept in an interoperable format… - **GDEZ, MDE, GDE, SKLM**

Art. 32 – The national authority may request agents of the public authorities to publish impact reports…- **GDPD, GDPF, GPBD, GDEZ, GA, GVA**

Art. 37 – The controller and the processor shall keep records of personal data processing operations…- **GA, GVA, DRM**

Art. 46 – Processing agents shall adopt security, technical and administrative measures able to protect personal data … **All**

Art. 49 – The systems used for processing personal data shall be structured in order to meet the security requirements- **All**

Legend:
Guardium Data Protection for Databases (GDPD), Guardium Data Protection for Files (GDPF), Guardium Data Protection for Big Data (GPBD), Guardium Big Data Intelligence (GBDI), Guardium Analyzer (GA), Guardium Vulnerability Assessment (GVA) - IBM Multi-Cloud Data Encryption (MDE), IBM Security Guardium Data Encryption (GDE), Guardium® Data Encryption for Db2® and IMS™ (GDEZ) - Data Risk Manager (DRM) - Security Key Lifecycle Manager (SKLM) - Data Security Services (DSS).

Use Cases

In the following use cases, it is helpful to understand these terms that are used. For the latest information and detail on terminology and meaning in the Brazilian General Data Protection Law (LGPD) policies, please visit the LGPD website and download the latest edition

I – **personal data**: information regarding an identified or identifiable natural person;
II – **sensitive personal data**: personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person;
III – **anonymized data**: data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing;
IV – **database**: structured set of personal data, kept in one or several locations, in electronic or physical support;
V – **data subject**: a natural person to whom the personal data that are the object of processing refer to;
VI – **controller**: natural person or legal entity, of public or private law, that has competence to make the decisions regarding the processing of personal data;
VII – **processor**: natural person or legal entity, of public or private law, that processes personal data in the name of the controller;
VIII – **officer**: natural personal, appointed by the controller, who acts as a communication channel between the controller and the data subjects and the national authority;
IX – **processing agents**: the controller and the processor;
X – **processing**: any operation carried out with personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction;
XI – **anonymization**: use of reasonable and available technical means at the time of the processing, through which data loss the possibility of direct or indirect association with an individual;
XII – **consent**: free, informed and unambiguous manifestation whereby the data subject agrees to her/his processing of personal data for a given purpose;
XIII – **blocking**: temporary suspension of any processing operation, by means of retention of the personal data or the database;
XIV – **deletion**: exclusion of data or a set of data stored in a database, irrespective of the procedure used;
XV – **international data transfer**: transfer of personal data to a foreign country or to an international entity of which the country is a member;
XVI – **shared use of data**: communication, dissemination, international transfer, interconnection of personal data or shared processing of banks of personal data by public agencies and entities, in compliance with their legal competences, or between these and private entities, reciprocally, with specific authorization, for one or more types of processing allowed by these public entities, or among private entities;
XVII –**impact report on protection of personal data**: documentation from the controller that contains the description of the proceedings of processing of the personal data that could generate risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms to mitigate the risk;
XVIII – **research body**: body or entity of the direct or indirect public administration or a nonprofit legal entity of private law, legally organized under the Brazilian law, with headqarter and jurisdiction in Brazil, that includes in its institutional mission or in its corporate or statutory purposes basic or applied research of historic, scientific, technological or statistical nature;
XIX – **national authority**: body of the indirect public administration responsible for supervising, implementing and monitoring the compliance with this Law.

Use Case 1: Building A Robust Cybersecurity Program

Section I - Security and Secrecy of Data, Art. 49 of the LGPD code mandates that a Processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing. In simple terms, it means to have systems in place doing everything they can to assess, avoid and alleviate cybersecurity issues before they can impact a user or consumer. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management should take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

Art. 49 - The systems used for processing personal data shall be structured in order to meet the security requirements, standards of good practice and governance, general principles provided in this Law and other regulatory rules. The monitoring and testing should include continuous monitoring or periodic Penetration Testing and vulnerability assessments." and as one key areas that must be accounted for, **Art. 32** - The national authority may request agents of the public authorities to publish impact reports on protection of personal data and may suggest the adoption of standards and good practices for processing personal data by the public authorities.

IBM sellers have the privilege of having one of the world's best solutions for addressing this space. IBM Guardium family or offerings is a clear market leader.. Whether it is a Vulnerability Assessment (Guardium Data Protection for Databases or Guardium Analyzer, IBM Data Security offerings provide comprehensive analyses that allow clients to address security concerns in a timely and efficient matter. And when integrated with the new IBM Big Data Intelligence and Guardium for Big Data companies have the foundation for a robust, highly scalable enterprise security monitoring solution that can consistently track vulnerabilities against policies and take appropriate action when issues are found.

Key Solutions:

- **IBM Guardium Analyzer**

○ IBM Security Guardium Analyzer efficiently finds LGPD-relevant data, understands data and database exposures, and acts to address issues and minimize risk.

- **IBM Guardium Vulnerability Assessment**

○ IBM Guardium Vulnerability Assessment scans data infrastructures (databases, data warehouses and big data environments) to detect vulnerabilities, and suggests remedial actions.

- **IBM Guardium Data Protection Solutions**

○ **IBM Guardium Data Protection for Databases:** ~~Assesses and monitors~~ Protects databases against attacks and data breaches via granular discovery, classification, ~~by automating security vulnerability testing~~ real-time monitoring and alerting, pre-built compliance policies and reports, and advanced analytics

○ **IBM Guardium Data Protection for Files:** Same as Guardium Data Protection for databases but for files (aka "unstructured data")

○ **IBM Guardium Data Protection for Big Data:** Same as Guardium Data Protection for Databases/Files, but for Big Data environments
○ **IBM Guardium Big Data Intelligence:** Enables customers to enrich their existing data security solution through creating an optimized security big data lake for improved agility, retention, and insights

Use Case 2: Processing of Children and Adolescents' Data

In the LGPD Section III focuses on Children's data and it's consent, use, validity and access to the data. Controllers of this data must take all precautions to identify and classify this data and keep it safe. **Art. 14** - The processing of personal data belonging to children and adolescents shall be done in their best interest, pursuant to this article and pertinent legislation. When processing data as mentioned in §1 of this article, controllers shall make public the information about the types of data collected, the way it is used and the procedures for exercising the rights referred to in Art. 18 of this Law. In addition and following **Art. 16** The personal data subject has the right to obtain the following from the controller at any time and by means of request. This includes: Confirmation of the existence of the processing, access to the data, correction of incomplete, inaccurate or out-of-date data, anonymization, blocking or deletion of unnecessary or excessive data or data, processed in noncompliance with the provisions of this Law. Using encryption of data and the eventual destruction of the keys when requested by the data data subject can provide a simple and complete solution to this code in **Art. 16**. in addition when you stop and consider that many breaches originate from outsourced vendors or service providers make sure your privileged access controls extend well beyond your direct employees. These 2 powerful solutions when combined create a strong line of defense for LGPD.

Key Solutions
IBM Guardium Data Protection Solutions
○ **IBM Guardium Data Protection for Databases and Files:** Assesses and monitors databases against attacks and data breaches by automating security vulnerability testing and real-time monitoring
○ **IBM Guardium Data Encryption solutions:** Encrypt data at rest across the enterprise and the cloud.

Use Case 3: Encryption of Personal Information

Art. 1 of the GDPF code states: This Law provides for the processing of personal data, including by digital means, by a natural person or a legal entity of public or private law, with the purpose of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person. **Art. 3** This Law applies to any processing operation carried out by a natural person or a legal entity of public or private law, irrespective of the mean, the country in which its headquarter is located or the country where the data are located. Much like the EU GDPR Regulation this law applies to any country that handles Brazilian Citizens Data. Protecting citizen data is a the core of this mandate.

Use Case 3: Encryption of Personal Information (cont.)

With the term processing be so broad; processing: any operation carried out with personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction. Encryption has become a must have for all your sensitive data. With key management standards like KMIP you can encrypt all of your data across all of your key self encrypting devices. Manage it all from a single simple administrative console. Encryption provides capabilities to help protect file and database data on-premises from misuse. In addition Separation of duties is mandatory so that administrators do not have free access to sensitive data. Cloud Data Encryption should include data access policies, integrated key management, sophisticated encryption and event monitoring, that all combine to deliver the scalability and flexibility to protect sensitive workloads regardless of where the data resides.

Key Solutions

IBM Guardium Data Encryption Solutions

○ **IBM Guardium for File and Database Encryption:** Encrypting file and database data helps organizations meet government and industry compliance regulations (including LGPD, PCI, the GDPR, NY DFS NYCRR 500, etc).

○ **IBM Multi-Cloud Data Encryption:** Helps meet compliance mandates for data protection, whether regulated or voluntary, as part of an overall cloud information security process.

○ **IBM Security Key Lifecycle Manager:** Centralizes, simplifies and automates the encryption key management process to help minimize risk and reduce operational costs of encryption key management.

○ **IBM Guardium for Tokenization:** Protects sensitive fields in databases and files with tokenization.

Use Case 4: Senior management Must Pay Closer Attention

More and more CEO's and their Board of Directors are being called into question about their lack of knowledge around security breaches and data loss prevention. Recently we saw a COE called before the US Senate Committee to answer questions about the company's misuse of customer data. Executives need a simple, easy to understand risk dashboard that allow them to make business risk decisions based on the latest accurate data, their jobs may depend on it. With new regulations like LGPD, GDPR and NY DFS NYCRR 500 Senior Executives must be more informed about their risks.

Key Solutions

○ **IBM Data Risk Manager:** Provides executives and their teams a business-consumable data risk control center that helps to uncover, analyze, and visualize data-related business risks so they can take action to protect their business.

Call Script & Prospecting Tools

Use the following Call Script as a guide. The goal is to engage in a conversation that specifically addresses how your client is complying with the data security aspects of the LGPD code.

After you begin the call with "*This is [name] from IBM Security,"* pause and wait a few seconds. If you know something specific about the person you are taking to then lead with that. For instance, perhaps they had a recent promotion or job role change or perhaps they put a recent posting on social media that you can leverage.

Next you will want to transition to a positioning statement relative to LGPD – something like this:

Rep: *I've been working recently with clients that have dealings with Brazilian Citizens and I have been helping them to implement data security solutions that comply with the new Brazilian General Data Protection Law (LGPD). Does that sound similar to what you are doing?*

If they are dealing with Brazilian Citizens in any capacity that requires compliance with LGPD regulations then they will have to prepare themselves to also comply with this new law. From this point you would like to have a short conversation with them about some of the key aspects as it relates to data security. Here are some good possible questions:

1.Do you believe your current Cybersecurity strategy does enough to protect the confidentiality, integrity and availability of your information systems?

2.Are you confident that you can quickly and correctly respond to a Cybersecurity event?

3.For the sensitive data that you are currently protecting,

1. Are you able to quickly identify and remediate vulnerabilities?
2. Are you able to perform continuous monitoring of your sensitive data to assess potential threats?
3. Are you able to conduct sufficient vulnerability testing to ensure confidence of the security of your production and test data?
4. Does your security staff have to spend a lot of time sifting through security alerts to remediate a vulnerability? Do they spend a lot of time chasing "false-positives"?
5. For the data that are outsourced and developed by third-parties are you able to ensure that your security policies for security are being followed and tracked?
6. Are you able to validate the security of your sensitive data assets?
7. Do you know exactly where all of your sensitive and regulated data resides, and what types of data you have? Are you continuously and automatically discovering and classifying that data as it is updated?

Once you have validated that there is an interest and need in data security, end the call by encouraging them to conduct a trial or see a demo of IBM Data Protection solutions. There are trials available for both on-premise and in the cloud.

LinkedIn InMail Script Best Practices:

Here's a summary of best-practice copywriting tips for composing your InMail:

- ✓ Use a compelling subject line. Referencing common interests or a specific challenge the prospect is facing are good starting points. Try to pique the prospect's curiosity.

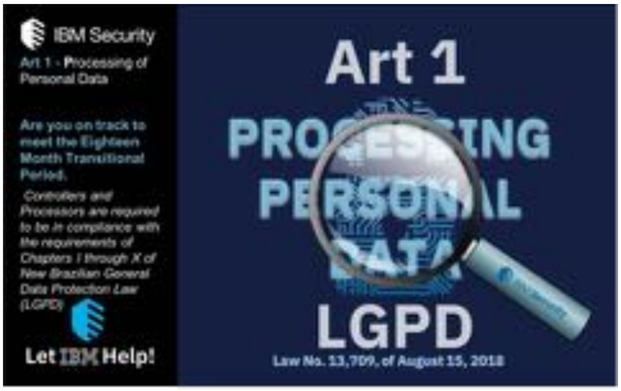
- ✓ Make it about them. Focus on benefits to the prospect, discuss their interests, and refer to awards or achievements noted on their LinkedIn profile to build rapport. Using inclusive language (“we” versus “I”) can also help.
- ✓ Start a conversation. Asking questions or sharing common details about your experience not only encourages a response, it shows you know what you’re talking about – whether it’s about a solution architecture or sports.
- ✓ Keep it short. The average online reader’s attention span is about eight seconds, so keep your messages to 100 words or so.
- ✓ Offer next steps. Always close with an action – either requesting a meeting or providing your availability for a conversation. This is the best way to ensure a response and start building the relationship further.

tip

When searching for prospects try the following key words:
Lei Geral de Proteção de Dados Pessoais, LGPD, Art., Art. 9 Access to Data, data privacy, vulnerability assessment, privileged user, Data Privacy Officer, Data Controller, Data Processor, Brazilian Data Protection Law, Covered Entity

Sample Social Selling LGPD Ads:

Send these forward with you InMail or Social Connects:



IBM Security

Art 1 - Processing of Personal Data

Are you on track to meet the Eighteen Month Transitional Period.

Controllers and Processors are required to be in compliance with the requirements of Chapters I through X of New Brazilian General Data Protection Law (LGPD)

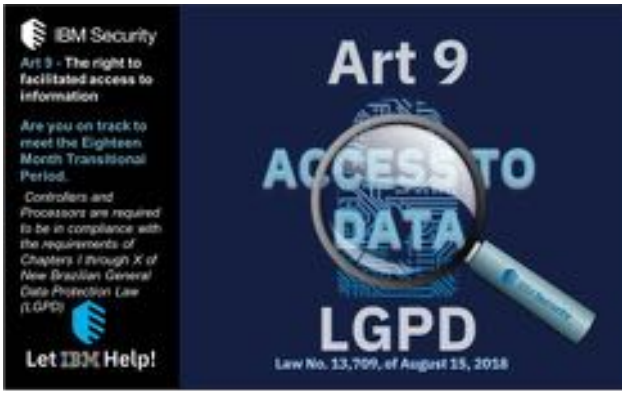
Let IBM Help!

Art 1

PROCESSING PERSONAL DATA

LGPD

Law No. 13,709, of August 15, 2018



IBM Security

Art 9 - The right to facilitated access to information

Are you on track to meet the Eighteen Month Transitional Period.

Controllers and Processors are required to be in compliance with the requirements of Chapters I through X of New Brazilian General Data Protection Law (LGPD)

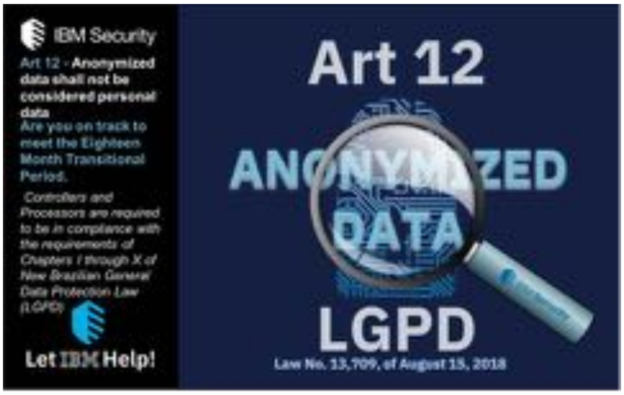
Let IBM Help!

Art 9

ACCESS TO DATA

LGPD

Law No. 13,709, of August 15, 2018



IBM Security

Art 12 - Anonymized data shall not be considered personal data

Are you on track to meet the Eighteen Month Transitional Period.

Controllers and Processors are required to be in compliance with the requirements of Chapters I through X of New Brazilian General Data Protection Law (LGPD)

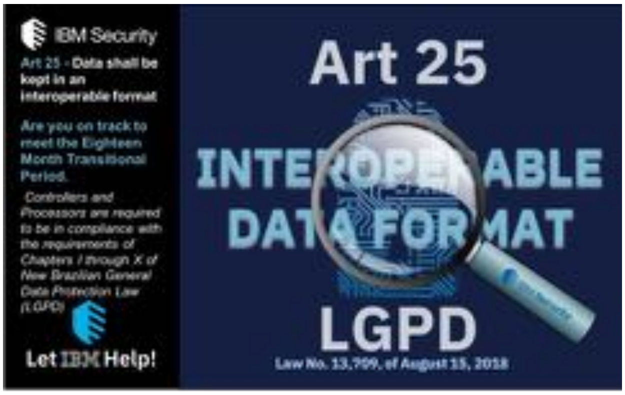
Let IBM Help!

Art 12

ANONYMIZED DATA

LGPD

Law No. 13,709, of August 15, 2018



IBM Security

Art 25 - Data shall be kept in an interoperable format

Are you on track to meet the Eighteen Month Transitional Period.

Controllers and Processors are required to be in compliance with the requirements of Chapters I through X of New Brazilian General Data Protection Law (LGPD)

Let IBM Help!

Art 25

INTEROPERABLE DATA FORMAT

LGPD

Law No. 13,709, of August 15, 2018

To Find more info contact: www.linkedin.com/in/glennafitzgerald or gafitzge@us.ibm.com:

Acknowledgments

The following resource was used to support this document

1. *Law No. 13,709, of August 14, 2018, https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf*

The following sections are parts of the LGPD Regulation, provided with commentary on how IBM Data Security fits with each.

Art. 46*: Processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing..*

IBM Security takes a holistic approach to protecting data and assets and believes that the future of security consists of Cloud, Cognitive and Collaborative capabilities coming together in an integrated and intelligent immune system. Much like a human's immune system, IBM has created the Security Immune System which organizes the various security capabilities around various respective domains and working as layers of defense—all working together to automate policies and block threats. This integrated and holistic approach includes data security and is centered around a cognitive core of security orchestration and analytics which continuously understands, reasons, and learns the many risk variables across the entire ecosystem of connected capabilities. IBM's capabilities also connect to an open partner security ecosystem of more than 100 ready for IBM Security partners.

Section III Good Practice and Governance: *Controllers and processors, within the scope of their competences, concerning processing of personal data, individually or in associations, may formulate rules for good practice and governance that set forth conditions of organization, a regime of operation, procedures, including for complaints and petitions from data subjects, security norms, technical standards, specific obligations for the various parties involved in the processing, educational activities, internal mechanisms of supervision and risk mitigation and other aspects related to the processing of personal data.*

IBM Data Security tools provide robust capabilities for vulnerability assessments and are specifically designed to be incorporated into continuous delivery processes and integrated together to better leverage automation. This section of the code also specifically mentions that these occur on an ongoing basis. However, these activities can delay the ability to release on time if they are done only in later development stages. Therefore, a key success factor today is being able to accomplish these kinds of tests on a continuous basis in order to identify and remediate vulnerabilities earlier in the development lifecycle. This is known as "shifting left" and is what allows organizations to balance the need for quality while still meeting goals for delivery and release speed,

Art. 50*:* d) establish adequate policies and safeguards based on a process of systematic evaluation of the impacts on and risks to privacy; h) are constantly updated based on information obtained from continuous monitoring and periodic evaluations;

IBM Data Security tools provide rich reporting and dashboard tools to quickly and easily allow visibility for vulnerability assessments. And by leveraging integrations into SIEM and other security and activity tracking tools (e.g. defect tracking systems, ticketing tools, file systems, etc) a robust auditing trail can be established – and even extended to include remediation efforts for a vulnerability. For instance – can your client locate a specific attack vector and set a threshold where if the threshold is exceeded the attacker can be locked down and quarantined as needed to prevent sensitive data loss. Addressing this quickly ultimately raises customer confidence and could avoid costly exposures.

Chapter VII, Security and Secrecy of Data: *When judging the severity of the incident, eventual demonstration that adequate technical measures were adopted to render the affected personal data unintelligible will be analyzed, within the scope and the technical limits of the services, to third parties who were not authorized to access them.*

Going beyond basic access controls to database instances. The rating process built into Guardium focuses on more sophisticated, dynamic, policy-based access management capable of identifying and removing excessive user privileges, managing shared and service accounts, and detecting and blocking suspicious user activities. It ability to monitor and enforce a wide range of policies, including sensitive data access, database change control, and privileged user actions makes it ideal for your LGPD compliance journey.

Section II Good Practice and Governance, Art. 50: *When establishing rules of good practice, the controller and the processor shall take into consideration, regarding the processing and the data, the nature, scope, purpose and probability and seriousness of the risks and the benefits that will result from the processing of data subject's data.*

As part of an overall Risk Assessment the Guardium Vulnerability Assessment and Guardium Analyzer Scans your data environment to detect vulnerabilities and suggest remedial actions. These solutions identify exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Full reports are provided as well as suggestions to address all vulnerabilities. Guardium Vulnerability Assessment detects behavioral vulnerabilities such as account sharing, excessive administrative logins and unusual after-hours activity. They help identify threats and security gaps in databases that could be exploited by hackers.

Art. 51: *The national authority shall encourage the adoption of technical standards that facilitate data subjects' control of their personal data.*

IBM Data Security solutions now contain cognitive capabilities that provide insight into vulnerabilities and risk. It reduced or eliminates false positives in security alerts and can be trained to identify variants that might spawn from a separate similar incident. This frees up your security staff to address more critical events and take a more proactive position around security.

Chapter V International Transfer of Data: *International transfer of personal data is only allowed in the following cases:*

I – to countries or international organizations that provide a level of protection of personal data that is adequate to the provisions of this Law

II – when the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided in this Law

IBM Security Services is a certified and qualified Third Party Service Provider to assist in complying with the requirements set forth in LGPD. Our security services provide cybersecurity personnel with cybersecurity updates and training more than sufficient to address relevant cybersecurity risks. With clients world wide and our X-Force threat detection services IBM is a world leader in enterprise security services

Chapter VII Security and Good Practices Section I, Security and Secrecy of Data: *When applying the principles mentioned in Items VII and VIII of the lead sentence of Art. 6 of this Law, and subject to the structure, scale and volume of her/his operations, as well as the sensitivity of the processed data and the probability and seriousness of the damages to data subjects*

IBM Guardium Data Encryption and IBM Multi-Cloud Data Encryption and our SKLM IBM Security Key Lifecycle Manager solutions can be used in part or as a wholistic solution to ensure encryption on-prem, in the cloud and across multiple cloud vendors while managing keys from a single administrative console throughout your enterprise. IBM Security Key Lifecycle Manager helps customers meet regulations such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPAA) and NY DFS NY CRR 500.15 by providing centralized management of encryption keys. IBM Guardium for File and Database Encryption provides encryption capabilities to help protect file and database data on-premises from misuse. In addition to file and database encryption, Guardium for File and Database Encryption also supports separation of duties, so that administrators do not have free access to sensitive data. Encrypting file and database data helps organizations meet government and industry compliance regulations (including PCI, the GDPR, etc). This offering performs encryption and decryption operations with minimal performance impact and high scalability for heterogeneous environments.

Summary: The Brazilian General Data Protection Law is very similar to the GDPR in context, structure and ultimate rational — to protect the fundamental rights and freedoms of natural persons, especially the development of natural persons' personality. However, its differences make the law unique and, in a way, more advanced than the GDPR, e.g, the inclusion within the scope of the law of anonymous data used for profiling purposes, a provision that it is in the heart of behavior analysis business models of all kinds. A lot is left to be explored but one thing is certain, citizen data will be protected around the world. Source: iapp, *Oct 4, 2018*