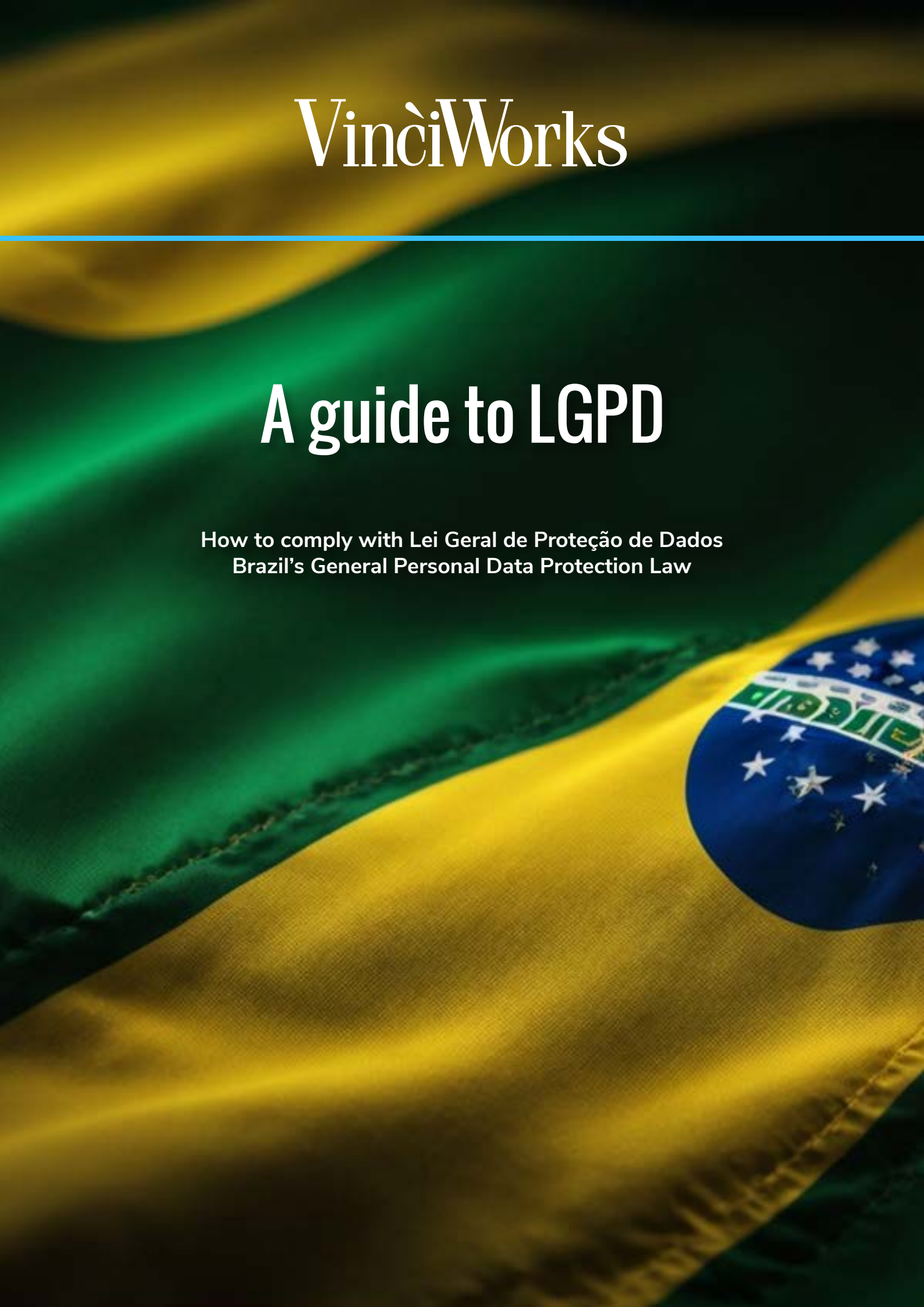
VinciWorks

A guide to LGPD

How to comply with Lei Geral de Proteção de Dados
Brazil's General Personal Data Protection Law



Introduction

Brazil's General Personal Data Protection Law (Lei Geral de Proteção de Dados or LGPD) entered into force in September 2020. It is the country's first comprehensive data protection law and aligns closely with the EU's sweeping data privacy act, the General Data Protection Regulation (GDPR).

Before LGPD, data privacy regulations in Brazil consisted of various provisions spread across Brazilian legislation. The aim of the LGPD was to unify the 40 different Brazilian laws that regulated the processing of personal data.

LGPD's focus is on promoting transparency and accountability in how personal data is managed by businesses. The law governs how businesses collect, process, store and use personal data. It applies to any business, no matter where they are located, that processes the personal data of anyone in Brazil. It makes no difference whether the data processing happens within Brazilian territory or not. The only relevant point is that the data subject is in Brazil.

Complying with LGPD is crucial for businesses handling the personal data of Brazilians. There are legal implications as well issues of consumer trust, data security, corporate responsibility, and preserving your business' reputation.

We recognise that understanding LGPD is vital for Brazilian companies as well as companies that want to facilitate cross border operations. We created this guide to ensure that companies have the information they need to do that.

A brief history of LGPD

Brazil has the largest economy in Latin America and is the 8th largest in the world. It is also increasingly garnering interest from businesses interested in global expansion. That means that businesses need to understand the country's data protection laws.

Before LGPD, Brazil's data protection laws were scattered across 40 different laws on privacy and data protection, creating a fragmented legal landscape and making it complicated for businesses wanting to do business in the country. These ranged from constitutional laws to civil codes to consumer protection laws to civil rights laws.

The state authorities decided to create a unified framework that would provide a comprehensive approach to data protection. In August 2018, the National Congress of Brazil enacted the LGPD.

LGPD took effect two years later, in August, 2020. The Brazilian government established the National Data Protection Authority (Autoridade Nacional de Proteção de Dados or ANPD) to manage the enforcement and ensure that data processors collect, use and share Brazilian residents' data in compliance with the LGPD.

Learn more

LGPD: An overview

LGPD sets forth Brazil's conception of personal data and when its use is authorised. Comprising 65 articles, it deals with the rights of data subjects and has 10 legal bases for the processing of personal data, which is four more than GDPR.

Key elements

Personal rights

LGPD gives individuals whose data is being collected and processed new rights. These include access to their collected personal data, its erasure, and data portability, which means that individuals have the right to access and transfer their personal information. Companies are required to comply with the requests within 15 days.

Data breach notification

Companies must notify the National Data Protection Authority about personal data breaches and the individuals whose data is affected must also be informed.

Data officer

Businesses are required to have a data protection officer (DPO) to oversee information processing.

Processing data

LGPD provides 10 principles for data processing and provides circumstances under which data can be processed, with consent at the top of the list.

Legal jurisdiction

LGPD applies to companies based in Brazil or those dealing with individuals in Brazil. If the company is headquartered outside Brazil, it must still comply with the data protection law when it comes to the country's citizens.

Learn more

Data mapping

Organisations are required to record all data processing activities and do a privacy impact analysis for personal data processing.

Penalties

The fines for non-compliance can reach up to 2% of a company's global revenue or US$9 million (R$44m).

Exceptions

The law does have a few exceptions, including national security, research, journalism and artistic purposes.

What is considered personal data?

Personal data is defined broadly in LGPD as *information regarding an identified or identifiable natural person.*

The law includes special restrictions for the processing of ***sensitive personal data.*** This is data that relates to:

- ✓ racial or ethnic origin
- ✓ religious beliefs
- ✓ political opinion
- ✓ affiliation to unions or political, philosophical or religious organisations
- ✓ health information
- ✓ sexual preference
- ✓ genetic and biometric data

Sensitive personal data may only be processed when the data subject specifically and distinctly consents to the specified purposes.

Personal data may be processed without consent for certain specific and limited purposes.

Learn more

Data subjects' rights

LGPD sets out nine fundamental rights granted to all Brazilian data subjects. These are a right to:

- ✓ Confirm that personal data is being processed
- ✓ Access to the data
- ✓ Correction of incomplete, inaccurate or out-of-date data
- ✓ Anonymise or delete data in some cases
- ✓ Request the transfer of data
- ✓ Delete personal data
- ✓ Receive information on how any personal data is being shared
- ✓ Be given information about the right not to consent to processing
- ✓ Revoke consent to processing

Learn more

Legal bases for processing data

Under LGPD, data is only to be processed under one of the legal bases that are specified in that law. In any other case, processing is prohibited.

Permissible bases for processing personal data are:

- ✓ With the data subject's consent
- ✓ Where required to comply with the data controller's legal responsibilities
- ✓ For the purposes of public administration and public policy as set out in relevant instruments
- ✓ For the purposes of research by a public entity
- ✓ data is to be 'anonymised' where possible
- ✓ Where necessary in accordance with a contract
- ✓ In order to exercise privilege in legal proceedings
- ✓ For the protection of life
- ✓ For the protection of health, by healthcare professionals
- ✓ In the 'legitimate interests' of the data controller or a third party, where there is not otherwise a breach of rights
- ✓ For the purposes of protecting a credit rating

Companies can collect and use publicly available personal data under the LGPD only if it is either:

being used for the same purpose that it was originally collected, in which case consent from the data subject is not needed

or

for a different purpose, but only if the controller has identified a valid legal basis for the use of the data

The data that companies collect and process can only be for the stated purpose and for the amount of time it's needed and the data must be stored securely.

Learn more

What else does my company need to know about LGPD?

Data mapping

In addition to identifying a legal basis for processing data without consent, companies must also create and maintain a map of the personal data that they collect and process. Organisations must also track consents and revocations by data subjects.

DPO

LGPD requires organisations to have a Data Protection Officer (DPO) but it does not outline specific cases for which a DPO is needed. It states that the "controller shall appoint an officer to be in charge of processing personal data." The understanding is that any organisation that processes the data of people in Brazil needs a DPO.

The DPO will be responsible for:

- ✓ Accepting complaints and communications from data subjects request and the National Data Protection Authority (Autoridade Nacional de Proteção de Dados, or ANPD)
- ✓ Training employees on best practices
- ✓ Other tasks as determined by the controller or indicated in complementary rules
- ✓ The Brazilian National Authority may indicate when the appointment of a DPO can be waived, based on the nature and size of the company or the volume of data processing operations

Learn more

Definition of consent

LGPD defines consent as the **"free, informed and unambiguous expression by which the data subject agrees to the processing of his personal data for a determined purpose."**

The law identifies conditions for obtaining, re-obtaining and proving receipt of consent, as well as conditions for revocation of consent.

Opt-in vs. opt-out

LGPD uses an opt-in model of user consent, which means that in most cases organisations cannot collect or process data until the user gives consent. This requirement includes both personal data like names and email addresses, but also granular data like that collected by website cookies.

Learn more

Who needs to worry about LGPD?

Any company anywhere that has data subjects in Brazil.

The law has a broad application. It includes any company that processes the personal data of individuals located in Brazil. The regulation's reach is not limited by the size of the business or the industry it operates in, nor is it confined to businesses physically located in Brazil.

The companies that must adhere to LGPD:

- ✓ Any company headquartered in Brazil, irrespective of where the actual data processing takes place, falls under LGPD jurisdiction.
- ✓ If a company collects, uses or processes the personal data of individuals located in Brazil, even if the business is not physically located in Brazil, it must comply with LGPD.
- ✓ If a company is not located in Brazil but it offers goods or services to individuals in Brazil, it must comply with LGPD.

From startups to multinational businesses, LGPD mandates that all companies processing Brazilian data subjects' personal data must adopt data protection measures in line with its provisions.

Learn more

Who will enforce LGPD?

LGPD creates the National Data Protection Authority (Autoridade Nacional de Proteção de Dados, or ANPD), an enforcement authority responsible for overseeing the data protection regulation. The ANPD has broad authority to create separate guidelines, rules and deadlines for small businesses and startups to make sure that they comply with LGPD.

LGPD does not give a firm deadline for reporting data breaches to the ANPD. It states that the controller must communicate to the national authority and to the data subject the occurrence of a security incident in a reasonable time period that is defined by the national authority.

How to report a data breach

If a data breach occurs, the controller must report it to the ANPD within a reasonable timeframe if it is likely to or has resulted in risk or harm to data subjects. ANPD guidance indicates that this information must be communicated within two working days of receiving knowledge of the incident.

Notifications need to include:

- ✓ a description of the nature of the affected personal data
- ✓ information about the data subjects involved
- ✓ information about the security measures that were in place
- ✓ risks created by the incident
- ✓ reasons for any delay in communication (if any)
- ✓ measures that have or will be adopted to address the breach and prevent a recurrence

The person or company responsible for the data must assess the incident and determine the nature, category, and number of data subjects affected.

The ANPD will verify the seriousness of incidents. It can require a company to adopt measures to safeguard data subjects' rights if necessary, including disclosure of the incident to the media, or measures to mitigate or reverse the effects of it.

Learn more

> Note: The ANPD may issue special rules and exemptions for LGPD for small businesses and startups. This would provide some flexibility for things like communication of security incidents to the ANPD and data subjects or deadlines for responding to data subjects' or the ANPD's requests.

The exceptions

Are there cases when LGPD does not apply? Yes, when the processing of personal data:

- ✓ is only for private and non-economic purposes
- ✓ is for journalistic, artistic, and/or academic purposes
- ✓ is for the purposes of public safety, national defence, state security or investigation and prosecution of criminal offences
- ✓ originates from outside of Brazil and is not the object of communication or shared with Brazilian data processing agents or the object of international transfer with another country other than the country of origin

Fines

Fines for noncompliance of LGPD is up to 2 percent of a company's annual revenue in Brazil, up to a maximum of about € 8.5 million per violation (R$ 44m).

The ANPD can also block access to data or further data processing, or require deletion of collected personal data. Individuals have the right to sue to seek civil damages for privacy violations.

Learn more

How is LGPD different from GDPR?

Both LGPD and GDPR are comprehensive data privacy and protection laws. But while LGPD was developed with GDPR in mind, there are some key differences between the two pieces of legislation.

- ✓ GDPR is more detailed than LGPD. For instance, in LGPD, the definition of personal data does not list examples of personal data. GDPR does. This gives regulatory bodies and the courts in Brazil more leeway in how they interpret these terms.
- ✓ Data subjects' rights are mostly similar but there are a few differences that could matter:

  > In GDPR, the right of data portability requires that the data be provided in a commonly used and machine-readable format. LGPD does not have this requirement.
  >
  > GDPR provides companies with a 30 day time limit to respond to access requests. LGPD gives only 15 days.

- ✓ LGPD has 10 legal bases for processing data while GDPR has six. This is largely because credit protection and research are not legitimate grounds for processing legal data in GDPR. This could mean that it will be easier for companies in Brazil to process personal data without seeking the consent of the data subject.
- ✓ In GDPR, the Data Protection Authorities (DPAs) are responsible for enforcing the regulation. They are set up within each EU member state and investigate GDPR breaches. Individuals and DPAs can take action both in national courts and the Court of Justice of the European Union (CJEU). In LGPD, enforcement is with the National Data Protection Authority (NDPA) but other government bodies such as public prosecutors or the National System of Consumer Defence can also bring civil or criminal cases to court. This could mean that there will be a lot of court action around LGPD and it could make it complicated to determine whose job it is to deal with LGPD's breaches.
- ✓ LGPD fines are not as substantial as GDPR.

Learn more

The benefits of compliance with LGPD

LGPD's main objective is to protect the rights of individual data subjects by promoting transparency and accountability in how their data is managed by companies. Compliance with LGPD is important for companies handling the personal data of people residing in Brazil. But the importance of compliance extends beyond its legal significance. It can have real implications for a company's overall business strategy, reputation and consumer trust.

Consumer trust

The way a business manages personal data can impact its relationship with consumers. Businesses that adhere to LGPD regulations transparently signal to consumers that they respect and protect their data. This can build a foundation of trust. Consumers are more likely to engage with businesses they can trust with their data.

Data security

Compliance with LGPD requires businesses to implement data protection measures such as securing personal data through encryption, anonymization and pseudonymization, ensuring the regular backup of data and preventing data breaches. This will improve a company's data security and reduce the risk of data breaches and cyber-attacks.

Cross-border operations

For companies looking to expand in Brazil, LGPD compliance provides a compliance framework that also aligns with other international data protection laws, such as the GDPR.

This can help a company's cross-border operations and reduce the risks that come with handling personal data across different jurisdictions.

Business reputation

Compliance with LGPD demonstrates that your company is taking data protection seriously and this commitment extends beyond consumers to how investors, partners, and stakeholders perceive the business. A company with strong compliance practices is seen as less risky, potentially attracting more investment and fostering better relationships with stakeholders.

Learn more

How can my company be compliant with LGPD?

Companies doing business in Brazil and subject to LGPD should:

- ✓ Delete customer data after the relationship ends
- ✓ Adopt technical and administrative data security measures to protect personal data from unauthorised access, accidents, destruction or loss
- ✓ Provide a data breach notification to both the data subjects and local authorities in case of a breach

Can my company transfer data out of Brazil?

The default rule is that companies cannot transfer data out of Brazil. But there are certain exceptions.

- ✓ The receiving country or organisation provides a level of data protection comparable to that of LGPD
- ✓ The non-Brazilian data importer is bound by a contract or by global corporate policy to provide and demonstrate a level of data protection comparable to that of LGPD
- ✓ There is international legal cooperation between government agencies
- ✓ The data subject has given specific consent to the transfer

Learn more

What to do now

Technology continues to evolve, and laws must evolve with them. Companies now need to prioritise compliance with data privacy, balancing it with revenue goals and fostering customer relationships. The risks of noncompliance are substantial, both in fines and reputation.

LGPD has a real impact on companies doing business in Brazil in a way that none of the previous 40 Brazilian privacy laws did. In light of the digital economy and the ever expanding use and role of personal data, companies in all sectors that want to do business in Brazil need to educate themselves on data privacy and protection and adapt their data collection practices to Brazil's LGPD.

Learn more

How VinciWorks can help

GDPR Compliance Training

Training is one of the key measures a company can take to ensure that staff comply with the regulation. But a one-off generic course is not enough. Training should be relevant and speak to each user's unique role and responsibilities.

Our gamified and interactive GDPR: Privacy at work course features a self-assessment tool that tailors the course to fit the learning needs of each employee in any role within the organisation. There are individually-designed modules for data protection critical areas of any business, including HR, marketing, consent rules, social media, Data Protection Officers responsibilities and the Data Protection Act 2018. In an age of ever growing data and privacy concerns, it's more important than ever to ensure all staff members have the latest training and understanding of data protection.

Learn more

Why VinciWorks?

Our suite of GDPR and data protection courses are packed with multiple course versions, realistic scenarios, and every customisation option you can think of. Our courses combine the latest in policy and law with best practice guidelines, providing real-world scenarios, interactive features, and review questions. Users will learn how to comply with data protection laws for their specific role in the organisation, and then have the chance to review and make sure they know how to apply the information.

Data Protection Training Courses

VinciWorks Data Protection Training materials will ensure your employees are equipped with the knowledge needed to keep your data secure. Course content covers issues such as:

- ✓ The 7 principles of Data Protection
- ✓ Data Protection legislation and how to comply with it
- ✓ Activities that could lead to a data breach and potential penalties
- ✓ Individual rights regarding personal data
- ✓ How to handle and process personal data securely
- ✓ Who has the responsibility for keeping information secure

We have several full length Data Protection courses and also offer a number of shorter supplementary courses which specialise in specific areas such as Binding Corporate Rules, Understanding and Securing Personal Data, and Information Requests.

Learn more

VinciWorks

Contact us

www.vinciworks.com

enquiries@vinciworks.com

+44 (0) 208 815 9308