Global Data Privacy and Cybersecurity Handbook - Brazil

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

Chapter updated as of January 2024.

New sector-specific regulations have been published by the Central Bank ("BACEN"), the National Telecommunications Agency (ANATEL), and the Civil Aviation Agency (ANAC) and they include relevant data privacy and cybersecurity obligations.

Further, the Brazilian Data Protection Authority (ANPD) published several relevant data protection documents in 2023, including enforcement actions, guidance, and regulations. ANPD also disclosed its Priority Themes Map for 2024 and 2025, which defines the themes for which official regulations from the ANPD are expected to be issued soon.

# Key Data Privacy & Cybersecurity Contacts

## Contacts



Trench Rossi Watanabe and Baker McKenzie have executed a strategic cooperation agreement for consulting on foreign law.

# Key Data Privacy and Cybersecurity Laws

## How are data privacy and cybersecurity laws/regulations implemented?

*Last review date: January 2024*

☒ omnibus – all personal data

☒ sector-specific — e.g., financial institutions, governmental bodies

Consumer protection, credit scoring, internet

☒ constitutional

## What are the key data privacy laws and regulations?

*Last review date: January 2024*

[Brazilian Federal Constitution](http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf)

According to the Brazilian Federal Constitution, one's right to personal data protection, intimacy, privacy, honor and image is a fundamental right and any violation of such right entitles the data subject to indemnification for both moral and material damages. The secrecy of correspondence, telegraphic, data and telephone communications is also guaranteed by the Constitution.

Article 5, X contains general provisions on the right to privacy.

Article 5, LXXIX was recently included by a constitutional amendment and establishes the protection of personal data as a fundamental individual right.

[Brazilian Civil Code - Law No. 10,406/02](http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm)

Article 21: Among other general provisions, it considers the right to privacy as a personality right, which cannot be waived or assigned as a matter of public policy.

[Brazilian Consumer Protection Code (CDC) - Law No. 8,078/90](http://www.procon.rj.gov.br/procon/assets/arquivos/arquivos/CDC_Novembro_2014_Ingles.pdf)

The CDC contains certain rules regarding the collection, storage and use of consumer data. The CDC regulates the creation of databases containing consumers' personal information. Under the CDC, a "consumer" is any individual or legal entity that acquires goods or services as an end-user. By this definition, the CDC governs not only retail sales to consumers, but also sales of products and services to legal entities that will be treated as consumers when and if they are end-users of products and services (on a case-by-case basis).

[Internet Legal Framework - Law No. 12,965/14](https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180)

Establishes general principles, warranties, rights and duties that govern the use of the internet in Brazil and regulates the protection of privacy and data online. It contains several provisions regarding internet users' rights to the protection of logs, personal data and private communications.

[Brazilian Criminal Code - as amended by Law No. 12,737/12](http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm)

Has general provisions addressing crimes relating to the inviolability of correspondence and the invasion of information technology devices.

[Interception of Telephone Communication Law - Federal Law 9,296/96](http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm)

Determines that an interception of phone calls may only be authorized by a judge in the context of a criminal investigation. The same rules apply to the wiretapping of information technology devices.

[Complementary Law No. 105/01](http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm)

Establishes rules regarding bank secrecy with which financial institutions must comply. Other sector-specific rules may also apply.

[Brazilian Information Access Law - Federal Law Nº 12,527/11](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm)

Regulates access to information held by public entities and agencies in Brazil, and also gives a legal definition of what is considered "personal information."

[Good Payer's Registry Law - Federal Law Nº 12,414/11, amended by Complimentary Law No. 166/2019](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm)

Regulates databases containing personal data related to credit and purchase history.

[General Data Protection Law ("**LGPD**")](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm)

In August 2018, Brazil passed Law Nº 13,709/18, which is the first omnibus data protection law in the country. The LGPD was amended by Law nº 13,853/2019, which, among other things, created the Brazilian Data Protection Authority.

The LGPD follows some of the concepts of the European General Data Protection Regulation (GDPR). Some of the key aspects adopted are the requirements for companies to **(i)** map all processing activities and maintain a record of processing; **(ii)** process personal data according to one of the legal bases for processing as set forth under the law; **(iii)** comply with data subjects rights; **(iv)** notify the authority and data subjects in certain cases of security incidents; **(v)** appoint a person in charge (equivalent, but not identical, to a data protection officer); **(vi)** adopt technical, organizational and security measures; **(vi)** and take additional steps in case of international data transfers. The law also sets forth different penalties that may be applied by the **ANPD**, including a fine of up to 2% of the group's net revenues in Brazil in the preceding year, limited to BRL 50 million (approx. USD 10.5 million).

It is important to remark that although the law is mostly inspired by the EU GDPR, it has a much simpler format and there are key differences including lower monetary penalties, shorter timeframes to comply with data subject access requests, and a specific legal basis for credit protection.

[Open Banking - Joint Resolution No. 01 of May 4, 2020](https://www.in.gov.br/en/web/dou/-/resolucao-conjunta-n-1-de-4-de-maio-de-2020-255165055)

Provides for the implementation of the Open Banking System. The Open Banking or open financial system is the right of customers of financial products and services to share their information and data among different institutions authorized by the BACEN and to move their bank accounts from different platforms (not only through the bank's application or website) in a secure, fast and convenient way.

## What are the key cybersecurity laws and regulations?

*Last review date: January 2024*

Apart from the laws and regulations mentioned in the section on Key Data Privacy and Security Laws, which may also have cybersecurity related provisions, the following are key cybersecurity laws and regulations in Brazil:

**FEDERAL LAWS**

[**Decree No. 9,573/2018**](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm)

Published on 23 November 2018, this Decree creates the National Policy for the Security of Critical Infrastructures and is applicable to the Federal Public Administration and state-owned companies dependent on resources from the National Treasury for the cost of personnel expenses or for general funding. Its purpose is to guarantee the security and resilience of Brazil's critical IT infrastructures. Some of its instruments are (i) the National Strategy for the Security of Critical Infrastructures, (ii) the National Plan for the Security of Critical Infrastructures, and (iii) the Integrated Data System on the Security of Critical Infrastructures.

It mainly aims to (i) prevent an eventual interruption, total or partial, of the activities related to the critical infrastructures, or, in the case of its occurrence, prevent the resulting impacts; (ii) establish guidelines and instruments to safeguard the critical infrastructure considered indispensable to national security; (iii) integrate data on threats, security technologies and risk management; (iv) identify interdependence relationships between critical infrastructures in the country; (v) develop, with a focus on prevention, an awareness of the safety of critical infrastructures; and (vi) establish the prevalence of the interest of defense and national security in the protection, conservation and expansion of critical infrastructures.

[**Decree No. 11,200/2022**](https://www.in.gov.br/en/web/dou/-/decreto-n-11.200-de-15-de-setembro-de-2022-430035293)

Published on 16 September 2022, this Decree creates the National Plan for the Security of Critical Infrastructures within the Federal Public Administration and is applicable to offices responsible for the Plan's strategic actions and dependent on resources from the National Treasury to fund personnel expenses or general funding. The Plan is one of the instruments of the National Policy for the Security of Critical Infrastructures, provided for in Decree No. 9,573/2018, and its purpose is to guarantee the security and resilience of Brazil's critical IT infrastructures.

Among other things, the Plan implements the Integrated System of Critical Infrastructure Security Data, the operational structure for the ongoing follow-up and monitoring of the Country's Critical Infrastructure Security, identified in various sectors

[**Decree No. 9,637/2018**](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm)

Published on 27 December 2018, this Decree provides for the implementation of the National Information Security Policy and is applicable within the Federal Public Administration. Its purpose is to ensure the availability, integrity, confidentiality and authenticity of information at the national level.

It mainly aims to (i) contribute to the security of the individual, society and the State, by guiding information security actions, observing fundamental rights and guarantees, (ii) encourage scientific research, technological development and innovation activities related to information security, (iii) continuously improve the legal and normative framework related to information security, (iv) promote the training and qualification of the human resources necessary for the area of information security, (v) strengthen the culture of information security in society, (vi) guide actions related to: (a) security of data held by public entities, (b) information security of critical infrastructures; (c) protection of the information of individuals who may have their safety or the safety of their activities affected, subject to specific legislation; and (d) processing of information with access restriction, and (vii) contribute to the preservation of Brazilian cultural memory.

[**Decree No. 10,222/2020**](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm)

Published on 6 February 2020, this Decree provides for the implementation of the National Cybersecurity Strategy and is applicable within the Federal Public Administration from 2020-2023. Its purpose is to make Brazil more prosperous and reliable in the digital environment, increase Brazilian resilience to cyber threats, and strengthen Brazilian cooperation in cyber security in the international scenario.

[**Decree No. 10,748/2021**](https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022)

Published on 19 July 2021, this Decree establishes the Federal Cyber Incident Management Network and is mandatory for offices and entities of the Federal Public Administration and voluntary for public companies and federal mixed-capital companies and their subsidiaries. Its purpose is to improve and maintain coordination between Federal, Municipal and States Public Administration entities, for the prevention, processing and response to cyber incidents, in order to improve the level of resilience in cyber security of the public entities in general.

[**Complementary Norm No. 08/IN01/DSIC/GSIPR**](https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=24/08/2010&amp;amp;jornal=1&amp;amp;pagina=1&amp;amp;totalArquivos=144)

Published on 23 August 2010, this Complementary Norm establishes the Guidelines for the Management of Incidents in Computing Networks in Federal Public Administration offices and entities and is applicable within the Federal Public Administration. Its purpose is to regulate the management of Security Incidents in Computer Networks by the Processing and Response to Security Incidents in Computer Networks Teams – ETIR of the Direct and Indirect Federal Public Administration offices and entities.

[**Complementary Norm No. 21/IN01/DSIC/GSIPR**](https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&amp;amp;jornal=1&amp;amp;pagina=5&amp;amp;totalArquivos=224)

Published on 8 October 2014, this Complementary Norm establishes the Guidelines for the Registration of Events, Collection and Preservation of Evidence of Security Incidents in Networks of offices and public entities which are part of the Federal Public Administration and, hence, is applicable within the Federal Public Administration. Its purpose is to establish guidelines for the recording, collection and preservation of evidence of security incidents in computer networks of offices and entities of the Direct and Indirect Federal Public Administration and the communication to the competent authorities, in order to allow for investigations of illegal conduct that damages or exposes the security of computer networks and systems or that may compromise the availability, integrity, confidentiality and authenticity of information in the Federal Public Administration.

[**The Digital Government Secretariat's Security Incident Response Guide**](https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_resposta_incidentes.pdf)

Published in December 2021, this Guide provides for good practices and guidelines for information security institutions and professionals to deal with cyber incidents, focusing on incidents involving personal data, and is applicable to professionals who are or will be assigned to the processing of personal data in various levels of the Federal Public Administration, as well as to the professionals responsible for the processing of cyber incidents in these institutions. Its purpose is to promote compliance with the **LGPD** within the Federal Public Administration.

[**Normative Ruling No. 5/21 of the Institutional Security Office ("GSI")**](https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684)

Published on 31 August 2021, this Regulation provides for the minimum information security requirements for the use of cloud computing solutions by bodies and entities of the Federal Public Administration and is applicable to all bodies or entities which are part of the Federal Public Administration that wish to use cloud computing. Its purpose is to regulate the safe use of cloud computing within the federal public administration.

**Decree 11,491/2023**

Published 12 on April 2023, this Decree ratifies the Convention on Cybercrime, signed by the Federative Republic of Brazil in Budapest on 23 November 2001. This International Convention harmonizes the laws of member countries on cybercrime, facilitating the member's co-operation in criminal investigations and with the dialogue on cybercrime.

**Decree 11, 856/2023**

Published on 26 December 2023, this Decree establishes the National Cybersecurity Policy and the National Cybersecurity Committee. The Decree aims to combat cybercrimes and malicious actions, promote the development of technologies for cybersecurity, and educate and empower society about cybersecurity. The committee was created to monitor the implementation and progress of the initiatives. The group will be responsible for monitoring and proposing actions to increase cybersecurity.

**STATE LAWS**

[**Regulation No. 9.908/2020 (State of São Paulo)**](https://www.tjsp.jus.br/Download/Portal/LGPD/Portaria_9908-20.pdf?637342337131143293)

Published on 20 August 2020, this Regulation redefines the Information Security Policy of São Paulo's State Courts and is applicable to judges, civil servants and outsourced workers who work at the São Paulo Court of Justice. Its purpose is to provide guidance, direction and support for information security in accordance with the business requirements and relevant laws and regulations.

[**Information Security Policy of the State of Rio Grande do Sul**](https://www.diariooficial.rs.gov.br/materia?id=669833)

Published on 27 January 2022, this Policy guides and establishes the corporate guidelines of the Secretariat of Justice and Penal and Socio-Educational Systems, for the protection of information assets and prevention of legal liability for all users of its computer network and is applicable to all users and service providers to the Secretariat's network. Its purpose is to (i) establish guidelines that allow users of the Secretariat's network to follow standards of behavior related to information security suited to the needs of their work activities and the legal protection of the Institution and the personal data of citizens; and (ii) guide the definition of standards and specific information security procedures, as well as the implementation of controls and processes for their compliance.

[**Normative Instruction Proderj/Pre No. 03/2022**](https://www.proderj.rj.gov.br/node/1084)

Published on 28 April 2022, this Normative Instruction regulates the information security procedures in Information and Communication Technology Solutions (ICT) to be adopted by the offices and entities integrating the direct and indirect administration of the executive branch of the State of Rio de Janeiro. Its purpose is to provide regulation of such procedures for the development, migration, support and security of websites and internet portals.

[**Normative Instruction PRODERJ/pre No. 01/2021**](https://www.proderj.rj.gov.br/node/1081)

Published on 26 February 2021, this Normative Instruction regulates the procedures for contracting and entering into agreements involving Information and Communication Technology Solutions (ICT) to be observed by the offices and entities that are part of Rio de Janeiro's Public Administration. Its purpose to provide regulation of such procedures and regulation regarding the sending of procedures for extending contractual instruments of this nature for analysis by PRODERJ (Information and Communication Technology Center of the State of Rio de Janeiro).

[**Resolution No. 03 of December 19, 2019**](https://ipeprev.rs.gov.br/upload/arquivos/202101/12094315-1576864345-resolucao-03-2019-psi.pdf)

Published on 3 December 2019, this Resolution provides for the Information Security Policy under the Institute of Social Security of the State of Rio Grande do Sul ("**IPE Prev**") and is applicable to users, managers and outsourced contractors. Its purpose is (i) regulate the use of Information and Communication Technology (ICT) resources, within the scope of the headquarters of the IPE Prev; and (ii) communicate good practices in the use of its resources, assuming the guarantee of confidentiality, integrity, authenticity, irreversibility and availability of information assets.

**SECTOR-SPECIFIC REGULATIONS**

**Banking**

[**BACEN's Resolution No. 4,893/2021**](https://www.in.gov.br/en/web/dou/-/resolucao-cmn-n-4.893-de-26-de-fevereiro-de-2021-305689973)

Published on 26 February 2021, this Resolution provides for the cyber security policy and the requirements for contracting data processing, data storage and cloud computing services, and is applicable to the institutions regulated by BACEN (except for payment institutions, which are regulated by Resolution No. 85/2021 - see below). Its purpose is to ensure the confidentiality, integrity and availability of the data and information systems used by such institutions.

[**BACEN's Resolution No. 85/2021**](https://www.in.gov.br/en/web/dou/-/resolucao-bcb-n-85-de-8-de-abril-de-2021-313194098)

Published on 8 April 2021, this Resolution provides for cyber security policies and the requirements for contracting data processing, data storage and cloud computing services, and is applicable only to payment institutions regulated by BACEN. Its purpose is to ensure the confidentiality, integrity and availability of the data and information systems used by such institutions.

[**Brazilian Securities and Exchange Commission Resolution ("CVM") No. 35 of 2021**](https://conteudo.cvm.gov.br/legislacao/resolucoes/resol035.html)

Published on 26 May 2021, the Resolution is applicable to entities and individuals that operate securities within the Brazilian stock market (intermediaries). It provides that intermediaries must (i) identify and list its relevant service providers; (ii) assess the controls performed by these service providers, and (iii) ensure that the service agreements with these providers: (a) comply with the obligation imposed by CVM to intermediaries of maintaining records re. certain data within a five-year period; (b) allows the regulated institution's access to the data and information be processed or stored by the service provider; and (c) ensures the confidentiality, integrity, availability and recovery of the data and information processed or stored by the service provider.

**BACEN's Regulation No. 304 of 2023**

Published on 20 March 2023, it approves the Regulation that governs, within the scope of the Brazilian Payment System, the operation of settlement systems, the exercise of the activities of registration and centralized deposit of financial assets and the constitution of liens and encumbrances on registered or deposited financial assets and consolidates rules on the matter. Although the regulation's main scope is not cybersecurity, it establishes certain cybersecurity obligations.

**BACEN's and National Monetary Council ("CMN") Joint Regulation No. 6 of 2023**

Published on 23 May 2023, the Resolution provides for requirements for sharing data and information regarding indications of fraud, to be observed by financial institutions, payment institutions and other institutions regulated by BACEN. According to the resolution, institutions authorized by BACEN to carry out financial activities will have to share information about indications of fraud with each other, with the aim of increasing the visibility of other players in this market about profiles that indicate a greater propensity to risk in commercial transactions. Therefore, every time a company in the financial sector identifies suspicious patterns or fraud attempts within its own system, it must report the incident so that it becomes available to other financial institutions, with the aim of strengthening the security of the payment ecosystem as a whole.

**BACEN's Regulation No. 338 of 2023**

Published on 23 August 2023, the Resolution establishes procedures for public entities to access data linked to Pix codes stored in the Directory of Transactional Account Identifiers (DICT), including confidentiality and purpose limitation obligations.

**BACEN's Regulation No. 342 of 2023**

Published on 26 September 2023, the Resolution amends the regulation governing the operation of the Pix payment arrangement (Pix Regulation) to include provisions on communication to data subjects in the event of security incidents involving personal data and on non-compliance with Pix's technical security requirements.

**BACEN's Regulation No. 412 of 2023**

Published on 26 September 2023, this Regulation establishes the operational procedures for communicating data subjects about security incident involving a database related to a Pix component or infrastructure. The Regulation establishes the obligation to communicate the incident to the data subject, even if the incident does not cause relevant risk or damage to the data subject.

**Insurance**

[**Superintendence of Private Insurances (SUSEP) Resolution No. 638/2021**](https://www.in.gov.br/en/web/dou/-/circular-susep-n-638-de-27-de-julho-de-2021-335760591)

Published on 3 August 2021, this Resolution provides for the cyber security requirements and is applicable to insurance companies, open private pension entities, capitalization companies and local reinsurers. Its purpose is to promote compliance with the provisions of the **LGPD** in the insurance market.

[**SUSEP's Resolution No. 171/2015**](https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/13866)

Published on 19 March 2015, this Resolution alters and consolidates the Information and Communications Security Policy of the Private Insurance Superintendence. The Information and Communications Security Policy's purpose is to establish strategic guidelines, responsibilities and competences, aiming to ensure integrity, confidentiality, availability and authenticity of the Private Insurance Superintendence's data and information against threats that could compromise its assets, including its institutional image.

**Energy**

[**Brazilian National Electricity Regulatory Agency (ANEEL) Resolution No. 964/2021**](https://www.in.gov.br/en/web/dou/-/resolucao-normativa-aneel-n-964-de-14-de-dezembro-de-2021-369359262)

Published on 22 December 2021, this Resolution provides guidelines and minimum standards for cyber security policies to be adopted by companies of the energy sector. Its purpose is to guarantee the security of the information, their technological structure and the privacy of customers' data.

**Telecommunications**

[**ANATEL's Resolution No. 740/2020**](https://www.in.gov.br/web/dou/-/resolucao-n-740-de-21-de-dezembro-de-2020-296152776)

Published on 24 December 2020, this Resolution creates a Cyber Security Regulation applicable to the telecommunication sector. Its purpose is to establish procedures to promote security in telecommunications networks and services, including cyber security standards and the protection of Critical Telecommunications Infrastructures.

[**Institutional Security Office (Federal Presidency) Normative Ruling No. 4/2020**](https://www.in.gov.br/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468)

Published on 27 March 2020, this Normative Ruling provides for minimum cybersecurity requirements that must be adopted in the establishment of 5G networks and is applicable to Federal Public Administration offices and entities in charge of implementing 5G networks. Its purpose is to increase the protection of society and national institutions, given the possibility of vulnerabilities and backdoors in 5G technology systems.

**ANATEL's Resolution No. 765/2023**

Published on 6 November 2023, the Resolution approves the General Regulation on Consumer Rights in Telecommunications Services. Consumers of services subject to this Regulation have the right to information on the measures applied by the telecom providers for the efficient and appropriate use of the services, especially those related to the management of their data, in addition to having the right to privacy in connection with billing documentation.

**Health**

[**Normative Ruling ANS/DC No. 501/2022 (National Supplementary Health Agency - ANS)**](https://www.legisweb.com.br/legislacao/?id=429817)

Published on 1 April 2022, this regulation establishes the Mandatory Standard for the Exchange of Information in Supplementary Health (TISS Standard) for health care data of beneficiaries of a Private Health Care Plan. The TISS is a mandatory framework for the electronic exchange of health care data belonging to health insurance beneficiaries, between private health care insurance providers that are not linked to the Brazilian Public Unified Health System (SUS). Its purpose is to promote the interoperability between the health information systems held by ANS and the Ministry of Health, as well as the reduction of information asymmetry for beneficiaries of private health care.

**Civil Aviation**

[**ANAC's Normative Ruling No. 128/2018**](https://pergamum.anac.gov.br/arquivos/IN2018-0128.PDF)

Published on 6 November 2018, this regulation provides for ANAC's cyber security policy and is applicable within the scope of the Agency, encompassing all servers, employees, suppliers, service providers and interns who officially carry out activities linked to institutional action and, where applicable, to the Agency's accredited agents, public or private bodies and entities. Its purpose is to provide the Agency with legal, normative and organizational instruments for scientific, technological and administrative training to ensure the confidentiality, integrity, authenticity, and the availability of data processed as classified and sensitive.

[**ANAC's Ordinance No. 5805/2021**](https://pergamum.anac.gov.br/arquivos/PA2021-5805.PDF)

Published on 30 August 2021, this regulation established the Information Security and Personal Data Protection Committee, whose responsibilities include, among others: issuing general guidelines to organizational units regarding the implementation of security actions for information and personal data protection, approving complementary norms related to information security and data protection and monitoring investigations and damages resulting from security breaches.

[**ANAC's "Cybernetic Security Awareness Manual in Civil Aviation"**](https://www.gov.br/anac/pt-br/assuntos/regulados/aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf)

Published on 9 August 2021, through Brazilian Aviation Security Team ("**BASeT**"), the "Cybernetic Security Awareness Manual in Civil Aviation" by ANAC provides general information and guidelines about cybersecurity for organizations and individuals interested in services provided in civil aviation. Its purpose is to help various civil aviation organizations and companies verify the security of internal processes that use information technology and assess the need for increased security. The information contained in the Manual can serve as a basis for carrying out cybersecurity risk assessments by aviation operators, required by regulations such as the Brazilian Regulation of Civil Aviation ("**RBAC**") No. 107 for airfield operators and RBAC No. 108 for air operators.

[**ANAC's "Use of the Cyber Security Assessment (ASC) Manual for Aviation"**](https://www.gov.br/anac/pt-br/assuntos/regulados/aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf)

Published in February 2023, through Brazilian Aviation Security Team ("**BASeT**"), the "Use of the Cyber Security Assessment (ASC) Manual for Aviation" aims to help organizations in the sector to assess their level of cybersecurity maturity and implement improvement measures. It provides a translation, with some adaptations, of THE CAP 1850 (Cyber Assessment Framework for Aviation Guidance) published by the UK Civil Aviation Authority. The experience undertaken by the United Kingdom was adapted to the Brazilian civil aviation sector to serve as a guidance and benchmark for Brazilian aviation companies.

## Are new or material changes to those key data privacy and cybersecurity laws anticipated in the near future?

*Last review date: January 2024*

Yes.

There are several Bills of Law aimed at changing the LGPD. They range from restrictions to the sharing of personal data by application providers with other legal entities or individuals to changes in the possible fines to be applied in cases of misconduct, among others. However, the most relevant regulations expected in the next 12 months are the regulations to be issued by **ANPD**.

Further, the AI Bill was proposed before the House of Representatives. There is no indication yet of when it will be analyzed, and if it will effectively become a law. In any case, if approved as is, it will create principles and guidelines for the development and application of AI systems in Brazil, including requirements for the processing of personal data by AI systems.

# Regulators and Enforcement Priorities

## Are there one or more data privacy and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: January 2024*

Yes.

Brazil has a federal-level regulator for LGPD matters, the ANPD. It was created as an entity associated with the Federal Presidency that has been associated with the Ministry of Justice as of January 2023 and has the authority to enforce the obligations provided under LGPD and to apply statutory penalties, such as fines and even prohibition to perform processing activities in the country.

However, the enforcement of data protection rights is not limited to the ANPD. Companies can also be subject to individual or collective claims from data subjects or other authorities or entities authorized to represent a class of data subjects including consumer authorities for failure to comply with the LGPD.

Also, as mentioned in the section "Key Data Privacy and Cybersecurity Laws," Brazil has several sector-specific regulations containing cybersecurity and data privacy provisions, issued by different authorities, such as BACEN, ANATEL, and CVM. Although such authorities are not properly data privacy/ cybersecurity regulators, non-compliance with their regulations, including its respective data privacy and cybersecurity obligations, may result in enforcement by such authorities against players of the industries subject to their regulatory framework.

## How active is each of the regulator(s)?

*Last review date: January 2024*

Consumer Authorities

☐ Not very     ☐ Moderately active     ☒ Very active

ANPD

☐ Not very     ☒ Moderately active     ☐ Very active

Sector-specific regulators

☒ Not very (for data protection and cybersecurity matters) ☐ Moderately active ☐ Very active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: January 2024*

The ANPD has been focused on the enactment of regulations to the LGPD.

Some of its key recent activities were the following:

ANPD published the Regulation on the Calculation and Application of Administrative Sanctions, which establishes standards and criteria for the application of administrative sanctions by the Authority, as well as the forms and dosimetry for calculating the base value of fine sanctions.

ANPD published a technical note on the processing of personal data in the pharmaceutical sector. It provides recommendations on the use of personal data in the pharmaceutical sector.

ANPD published a Q&A outlining proper procedures for preparing Data Protection Impact Assessments (DPIA).

ANPD published a statement on the processing of personal data of children and adolescents. In the statement, the Authority provided an interpretation of the provisions of the LGPD on the topic.

ANPD published a preliminary study on the application of legitimate interest as a legal basis for processing, including some guidance for the conduction of the LIA (legitimate impact assessment).

ANPD published Guidelines on Processing Personal Data for Academic Purposes, which aims to aims to clarify doubts about the legal basis that allow the processing of personal data for such purpose and the provision of access to or sharing of personal data for the purposes of studies and research.

ANPD released an updated version (Version 2.0) of its Guidelines for the Processing of personal data by Public Authorities. The updated version of the document aims to establish objective parameters to help organizations and public bodies to implement the LGPD.

ANPD published a draft resolution on requirements related to security breaches, which was open for public consultation until June 2023. The aim of the draft Resolution is to regulate the requirements for controllers to report security incidents that may cause significant risk or damage to personal data subjects. The proposed regulation also specifies the deadline for notifying the ANPD.

ANPD released a draft resolution on requirements related to the "person in charge" (DPO equivalent - although not identical), which was open for public consultation until the beginning of December 2023.

ANPD published a draft for Standard Contractual Clauses (SCCs) and also launched a public consultation on requirements for international data transfers, which was open for public consultation until the beginning of October 2023.

As such, enforcement of the topics above may be expected in the near future.

ANPD also disclosed a Priority Themes Map for the years of 2024 and 2025, which defines the topics and priorities of ANPD’s work, defining the objectives and monitoring parameters and also the dates for which the regulations are expected.

Data subject rights is the first topic that the Authority expects to regulate, between the first semester of 2024 and the second semester of 2025. The main goals are to conduct enforcement actions, publish guidance and preventive actions, within the scope of data processing by the public authorities, digital platforms, the financial sector and the telecommunications sector.

Processing of minors' data is the second theme the Authority expects to regulate. For this topic, regulations are expected to be issued between the second half of 2023 and the second half of 2025.

Artificial Intelligence is the third topic that the Authority expects to regulate. It estimates regulations to be issued in the first half of 2025. The purpose is to identify potential risks in the processing of personal data in the context of facial recognition systems and to ensure compliance with the LGPD in regard to the processing of biometric data.

Data scraping is the fourth topic that the Authority expects to regulate. The main goal is to verify processing activities involving data scraping to assess any need for appropriate measures to comply with the LGPD's obligations.

# Key Definitions

## Personal data

*Last review date: January 2024*

LGPD defines personal data as "any information related to a natural person identified or identifiable" (article 5, I).

The Constitutional protection of privacy and the provisions of the Civil Code are very broad as they refer to the protection of the individual's privacy, intimacy, and personal data. The CDC refers to any information included in registrations or forms and any data regarding the acquisition of products or services.

Decree No. 8,711/2016, which regulates the Internet Legal Framework, provides a definition of Personal Data which, in theory, is limited to the purposes of such law. The Decree defines Personal Data as any data related to an identified or identifiable individual, including identification numbers, location data or electronic identifiers when these are related to a person.

Furthermore, the Brazilian Information Access Law defines personal information as any information regarding an identified or identifiable individual. This definition may be used as a reference point for the purposes of data protection laws and is generally adopted in courts and by scholars when addressing this matter.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: January 2024*

Sensitive data includes:

☒        personal data revealing racial or ethnic origin

☒        personal data revealing political opinions

☒        personal data revealing religious or philosophical belief

☒        personal data revealing trade / professional union or association membership

☒        genetic data

☒        biometric data for the purpose of uniquely identifying a natural person or biometric templates

☒        data concerning health/medical information

☒        data concerning a natural person's sex life or sexual orientation

☐        financial information

☐        government identity card or number information

☐        personal data regarding an individual's criminal convictions or record

☐        passwords

☐        other

## Controller vs Processor

*Last review date: January 2024*

**Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:**

the controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

the processor/agent is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

**Answer:** Yes

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: January 2024*

☒        applies to organizations located in the jurisdiction

☒        applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction

☒        applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction

☐        no express territorial scope, but would require some nexus to the jurisdiction

☒        other

applies to processing of personal data collected in Brazil

# Information Requirements

## What information needs to be included in a privacy notice to data subjects?

*Last review date: January 2024*

☒        the identity and the contact details of the controller and, where applicable, of the controller's representative

☒        the contact details of the data protection officer, where applicable

☒        the purposes of the processing for which the personal data is intended

☐        the legal basis for the processing

☒        the categories of personal data concerned

☐        the source from which the personal data originates, and if applicable, whether it came from publicly accessible sources

☒        the legitimate interests pursued by the controller or by a third party if processing is based on the legitimate interests ground

☒        the recipients or categories of recipients of the personal data, if any

☒        information regarding data transfers to third countries, where applicable, and reference to appropriate or suitable safeguards and the means by which by to obtain a copy of them or where they have been made available

☒        the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

☒        the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.

☒        the existence of the right to withdraw consent if processing is based on consent

☒        how the data is held

☒        the security provided to the data

☒        the right to lodge a complaint with a supervisory authority

☐        whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

☒        if applicable, information regarding automated decision making, including profiling

☒        other

Identity and contact detail of the Person in Charge, where applicable (according to the LGPD, it should be published preferably on the company's website)

Also, in one specific case, the ANPD commented that it would be desirable to disclose the legal basis for processing. But we remark it was an isolated case and there are no consolidated legal precedents in this regard.

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: January 2024*

The following are potential legal bases for processing personal data:

☐        appropriate notice has been provided to or made available to the data subject

☒        the data subject has provided consent to the processing for the identified purposes

☒        the personal data is necessary to perform a contract with the data subject

☒        the personal data is necessary to comply with a legal obligation

☒        the personal data is necessary to protect the vital interests of a natural person

☐        the personal data is necessary for a public interest

☒        the personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject's privacy interests and the data subject has not made use of his/her right to object)

☒        other

Under Article 7 of the LGPD, the following are additional legal bases to process non-sensitive data:

The personal data is necessary for the performance of public policies by the public administration (government bodies)

The personal data is necessary for the performance of studies by research organizations, and, when possible, the personal data should be anonymized

The personal data is necessary for the regular exercise of rights on legal, administrative or arbitral action

The personal data is necessary for the protection of health, on proceedings performed by healthcare professionals or by health entities

The personal data is necessary for credit protection

# Legal Bases for Processing of Sensitive Data

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: January 2024*

☒ Yes     ☐ No     ☐ No, but additional legal bases are necessary

The following are potential legal bases for processing special categories of personal data:

☐        the data subject has given consent to the processing, where consent is measured to the same standard as non-sensitive personal data

☒       the data subject has given consent to the processing, where consent is measured to a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")

☐        processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

☐        processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

☐        processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions

☐        processing relates to personal data which are manifestly made public by the data subject

☒        processing is necessary for the establishment, exercise or defense of legal claims

☒        processing is necessary for reasons of substantial public interest

☒        processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

☒        processing is necessary for reasons of public interest in the area of public health

☐        processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

☒        other

Article 11 of the LGPD sets forth separate legal bases to process sensitive data, as follows:

a. Free, informed and unequivocal consent by data subject, and such consent must be specific and highlighted, and shall refer to specific purposes; or

b. Without consent from data subject, where it is required for:

Compliance with legal or regulatory obligation by the data controller

For the shared processing of data as required by public administration to carry out public policies that are set forth in laws and regulations

For research institutions to conduct studies and research, in which case the anonymization of sensitive data should be guaranteed whenever possible

For the regular exercise of rights, including in contracts and in lawsuits, administrative proceedings or arbitration

For the protection of life or physical integrity of data subject or third parties

For the protection of health, solely in proceedings carried out by health professionals or health services, or

To prevent fraud and guarantee the security of data subjects in proceedings for identification or authentication in electronic systems, provided that data subjects' rights are protected, and except in case the fundamental rights and freedoms of data subjects prevail to require the protection of personal data.

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: January 2024*

Yes.

**The potential legal bases for data processing in the employment context are:**

Same as the processing of personal data outside the employment context. But generally speaking, the most commonly used legal bases are compliance with a legal obligation, performance of a contract and legitimate interests (the last one is for non-sensitive data only).

## Can consent be validly obtained in the employment context?

*Last review date: January 2024*

☐       Yes, same as for data subjects outside the employment context.

☒       Yes, but this consent is typically more difficult to establish in an employment context (specify details below)

☐       No

To date, there are no specific guidelines addressing this matter. Similar to the GDPR, consent given in the context of employment relationships can be challenged in light of the LGPD. This is because the LGPD establishes that consent must be freely given, and there is a risk that consent given by an employee will not be deemed "free" for such purposes, given the subordination and unbalanced relationship between employer and employee. To increase the chances of consent being deemed valid, the employee must be truly free to choose whether or not to give consent (i.e., employee's failure to give consent should not give rise to any penalties, sanctions, disadvantages or otherwise negative consequences).

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

☐        Yes

☒         No

ANPD has issued two analyses on the AI Bill which provides for the regulation of the use of artificial intelligence (AI) in Brazil. However, it has not mentioned anything specific about the use of artificial intelligence, automated decision-making or profiling in an employment context.

If yes, please provide a link.

# Minors

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: January 2024*

Yes.

A minor within the meaning of data privacy laws is a person below the age of 18.

The LGPD establishes specific requirements for the processing of data from children and adolescents.

According to Brazil's Child and Adolescent Statute, a child is any person up to 12 years of age, and an adolescent is any person between 13 and 18 years of age. Therefore, both are considered minors for purposes of the law, and the LGPD imposes special requirements in relation to personal data of minors.

According to the Brazilian Civil Code, only individuals over the age of 18 are capable of binding themselves personally. Minors under 16 are considered absolutely incapable, while those between 16 and 18 are considered relatively incapable (i.e., they can bind themselves with the assistance of their parents or guardians).

In 2022, the ANPD has published a preliminary study on legal bases applicable to the processing of personal data of minors. In this study, the ANPD asserted that the legal bases provided for in Articles 7 (legal bases for the processing of personal data) and 11 (legal bases for the processing of sensitive personal data) of the LGPD could be applied to the processing of data from minors, provided that data such processing meets the minors' best interests, what should be assessed on a case-by-case basis.

Recently, the Authority also published a statement on this matter, providing a standardized interpretation on the application of legal bases for the processing of children's and adolescents' personal data. According to the Authority, processing of minors' data can be based on the legal bases provided in Articles 7 and 11 (i.e., general legal bases for the processing of non-sensitive and sensitive personal data), as long as the minors' best interests are observed (to be assessed on a case by case basis).

## In what circumstances do these special requirements apply?

*Last review date: January 2024*

☒        generally
☐        in the context of information society services only if processing is based on consent
☐        in the context of educational services
☐       other

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: January 2024*

☐       consent must be given or authorized by the holder of parental responsibility over the child
☒       additional data subject rights are granted to minors (e.g., deletion, access, transparency)

Controllers must process personal data of children and adolescents only in their best interests, and must make information about the data categories collected, the use of such data and the proceeding to exercise data subject rights publicly available.

Furthermore, the information about the data processing must be given in a simple, clear and accessible way, considering the physical, perceptive, sensorial, intellectual and mental user characteristics. The use of audio-visual resources may be appropriate in some instances and parents or legal representatives must be provided with the necessary information.

☐       additional data security requirements apply
☒       other

Where consent is required, personal data relating to children may be collected without consent if the collection is necessary to contact the parents or legal representative and the personal data is used only once and is not stored, or for the child's protection. In this scenario, personal data cannot be transferred to third parties without consent.

The data controller must not make data subject's participation in games, internet applications and other activities conditional upon the provision of personal data beyond what is strictly necessary for participating in the activity.

Where consent is needed, the data controller must perform every reasonable effort to verify whether the consent was given by the child's representative, considering the available technologies.

# Data Subject Rights

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: January 2024*

Yes.

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒        right to access the data subject's own personal data
☒        right to rectify/correct the data subject's own personal data where inaccurate or incomplete
☒        right to erasure of personal data
☒        right to restrict data processing
☒        right to data portability
☒        right to object to the processing of personal data
☒        right to withdraw consent
☒        other

Right to ask for data to be anonymized

Right to lodge a complaint before the ANPD

Right to obtain a copy when the legal basis for processing is consent or performance of a contract

Right to anonymize, block or delete unnecessary or excessive personal data, or data processed without compliance with the LGPD

Right to be informed about the public and private entities with whom the data has been shared

Right to review decisions made solely on the basis of automated processing

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: January 2024*

Yes.

The restrictions or requirements are as follows:

☐       absolute right not to be subject to a decision based solely on automated decision making, including profiling
☐       qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them
☐       right to information / transparency requirement
☐       right to request human review of the automated decision making
☐       data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her
☒       other

The data subject has the right to request the review of decisions taken solely based on the automated processing of personal data which affects their interests, including decisions aimed at defining their personal, professional, consumption and credit profiles or aspects of their personality.

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: January 2024*

No.

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: January 2024*

☐        Yes

☒         No

***If yes, please provide brief details and a link.***

ANPD recently published two preliminary studies on the AI Bill that aims at regulating the use of AI in Brazil). However, these studies are not binding, and focuses on the proposed AI Bill and ANPD's role on the enforcement of AI requirements as a regulator of data protection matters, instead of on actions that companies should take in order to implement AI Systems (such as automated decision-making or profiling requirements).

## Do other (non-privacy or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: January 2024*

☐       Yes, laws in force

☐       Draft legislation in progress

☒       Proposal for legislation or regulation at an early stage

☐       Non-binding guidance or principles issued or in progress

☐       No, nothing in force or in progress

***If yes, please provide brief details and a link.***

An AI Bill has been proposed before the House of Representatives, which aims to create rules for AI systems to be made available in Brazil, establishing the rights of those affected by their operation. The bill pertains to the use of automated decision-making and establishes specific rights for those affected by these decisions. According to the Bill, people affected by an artificial intelligence system will have the right to challenge and request review of decisions, recommendations or predictions generated by such a system that produce relevant legal effects or that significantly impact their interests.

It defines the criteria for the use of these systems, including by the public authorities, providing for penalties for any violations of the law and also provides the creation of an authority that will oversee and regulate this subject matter. For instance, the Bill requires companies to conduct risk assessments before launching a product or service that applies AI techniques and divides the risk levels into AI systems of excessive risk and AI systems of high risk.

AI systems classified as "Excessive Risk" are expressly prohibited. AI systems classified as "High Risk" should be subject to an algorithmic impact assessment. The Bill provides some criteria for companies to assess whether the AI system is considered as excessive or high risk.

# Data Protection Officers

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: January 2024*

Yes. There is the concept of a "person in charge," which is a DPO equivalent (though not identical).

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

☒        the processing is carried out by a public authority or body, except for courts acting in their judicial capacity

☒       the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

☒       the core activities of the controller or the processor consist of processing on a large scale of special categories of data

☒       the organization employs more than a certain number of individuals in the jurisdiction

☒       other

Per Article 41 of the LGPD, all data controllers must appoint a person in charge (DPO equivalent). However, in January 2022, the ANPD issued Resolution CD/ANPD No. 02, which removed the requirement to appoint a person in charge for micro and small companies, start-ups, the self-employed and non-profit associations. While not mandatory, such appointment will be considered good practice.

Regarding this matter, the ANPD also published the draft of a regulation aiming to establish complementary rules on the appointment, definition and duties of the person in charge. Such draft was open for members of the society to provide suggestions until the beginning of December. The ANPD is currently analyzing the suggestions and shall enact a formal regulation soon.

The draft resolution provides more details about: (i) formal requirements on the appointment of the "person in charge"; (ii) personal attributions that the person in charge should meet; (iii) which information about the person in charge's identify must be publicly disclosed; (iv) the responsibilities and activities that the "person in charge" should perform; (v) the cases in which there may be a conflict of interest in the appointment of the person in charge.

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: January 2024*

Yes

If yes, what are these requirements?

☐       legal qualifications / experience

☐       other professional qualifications / experience

☐       resident in the jurisdiction

☒        other

The law establishes that the identity and contact information of the person in charge must be publicly disclosed, clearly and objectively, preferably on the company's website.

Additionally, the aforementioned draft resolution made open for public consultation may create further requirements, if published as per its current draft. For instance, it provides that the appointment of the person in charge must take into account their professional qualities and, above all, their knowledge of the subject of privacy and data protection.

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: January 2024*

Yes.

The obligations are as follows:

☐       controllers must conduct due conduct diligence on the processor to ensure it will provide appropriate security and processing of the personal data
☐       controllers must only use processors subject to a written agreement that complies with specific requirements
☒       other

Controllers must provide to the processor instructions regarding the processing of personal data and verify the Processor's compliance with their instructions and with the applicable laws.

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: January 2024*

Yes.

Per Article 37 of the LGPD, the data processor must keep a record of the personal data processing operations they perform.

# Notification, Filing, Registration & Approval Requirements

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: January 2024*

No.

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: January 2024*

Yes.

Any country that is not Brazil.

Transfers of personal data to third countries are only permissible if there is a legal basis for the processing/transfer and one of the following applies:

☒       approved adequate/whitelisted jurisdictions
☒       to holders of specific certifications or followers of specific code of conduct programs each approved by the relevant data protection and cybersecurity authority (e.g., EU-US Data Privacy Framework)
☒       approved standard contractual clauses
☒       binding corporate rules
☒       derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims
☒       other solutions

As per Article 33 of the LGPD, other transfer mechanisms available include:

When the transfer is necessary for international legal cooperation between public intelligence agencies, public investigation agencies and public prosecution agencies, in accordance with international law mechanisms

When the transfer is necessary for the protection of the life or physical safety of the data subject or a third party

When the ANPD authorizes a specific transfer

When the transfer is a product of a commitment undertaken under international cooperation

The ANPD recently launched a public consultation on the regulation of international transfers of personal data. The draft was open for public consultation until October 2023. The ANPD is currently analyzing the suggestions and will enact a formal regulation on the topic soon. As a highlight, the draft provides a draft of the Standard Contractual Clauses (SCCs).

# Data Localization/Residency

## Are there data localization / data residency or other types of laws that may require the retention and storage of personal data in the local jurisdiction?

*Last review date: January 2024*

No.

☐       Data localization / data residency laws that mandate retention of personal data or a copy thereof in the local jurisdiction (include whether copies or the original data may also be stored outside of the jurisdiction):

☐       Other laws that may require the retention and storage of personal data (including, for example, where such data is part of another type of record or dataset) in the local jurisdiction or otherwise prohibit the transfer or disclosure of the personal data outside of the local jurisdiction:

☐        national security laws

☐        anti-investigatory/blocking statutes that restrict any activity on local territory that aids a foreign government investigation

☐        tax or financial record laws

☐        employment laws

☐        export control laws

☒       other

While there are no general data residency/localization obligations, there may be such data residency/localization requirements if classified State information (not limited to personal data), or data related to the Federal Public Administration is processed.

Moreover, BACEN's Resolutions No. 4,893/2021 and No. 85/2021 provide certain data residency requirements for cloud service providers.

# Security Requirements

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: January 2024*

Yes.

☒        general obligation to take appropriate / reasonable technical, physical and/or organizational security measures
☒        obligation to take specific security measures e.g., encryption
☐       requirement to undertake third party due diligence (security assessment of third party providers)
☒       other

According to Article 46 of the LGPD, an organization is required to take steps to: (i) ensure that personal data in its possession and control are protected from unauthorized access and use; (ii) implement appropriate physical, technical and organization security safeguards to protect personal data; and (iii) ensure that the level of security is in line with the amount, nature, and sensitivity of the personal data involved.

The ANPD may create additional security standards.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: January 2024*

Yes.

☒       public company obligations (e.g., duties to maintain sufficient information security measures or ensure operational resilience to cyberattacks)

☐       network information security requirements (broader than telecommunications)

☒       health regulatory requirements

☒       financial services requirements

☒       telecommunication requirements

☒       providers of critical infrastructure

☒       other

Insurance and Civil Aviation sectorial regulation.

**If yes, please provide brief details of the relevant law or regulation.**

Please refer to our answer to the question "What are the key cybersecurity laws and regulations?"

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

☒      Data privacy

☐      Securities or public company

☐      network information security

☐      health

☐      financial services

☐      telecommunications

☐      critical infrastructure

☐      other

The main regulatory guidance and public statements made by the ANPD are mentioned in the section: "What are each of the regulator's anticipated enforcement priorities for the next 12 months?"

Regarding enforcement actions, the Authority recently issued its first sanction for non-compliance with the LGPD. According to ANPD, the company violated articles 7 and 41 of the LGPD, and article 5 of the ANPD's regulation No. 1 of 2021.

The Authority also recently issued two penalties against two public bodies. In the first penalty, the ANPD's coordination fined the public body Assistance Institute for State Public Servants of São Paulo (IAMSPE) for allegedly violating Article 49 of the LGPD. The second penalty was issued against the Santa Catarina State Health Department (SES-SC), for allegedly infringing Article 49 of the LGPD. Breach Notification Requirements.

# Breach Notification Requirements

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: January 2024*

Yes.

There is an obligation to notify the ANPD and data subjects of any breach that may result in relevant risk or damage to the data subject. Yet, the law does not define what would be a relevant risk or damage to the data subject, and there is very limited guidance provided by the Authority. Sectorial regulations also set forth specific data security breach notification requirements.

Recently, the ANPD published the draft for a regulation on data security breaches, which was open for public consultation until June 2023. The regulation aims to provide requirements for the controller to report data breach incidents that may cause significant risk or damage to personal data subjects, pursuant to Article 48 of the LGPD. The ANPD is currently reviewing the contributions of members of the society to the draft regulation, and an official regulation about the matter is expected to be issued soon.

## Controllers/ Owners have to notify:

*Last review date: January 2024*

☒       data protection authorities

The communication must be made in a reasonable time. The ANPD has only published a preliminary and non-binding form for online breach notification. Such form indicates as reasonable time a period of two business days, counted from when the controller became aware of the incident. However, if the aforementioned draft regulation from the ANPD regarding the data security breaches is approved as is, the timeline may be changed to three business days.

☐       cybersecurity authorities

☒       affected individuals

Same as above.

☐       other

## Processors/ Agents have to notify:

*Last review date: January 2024*

There are no legal requirements for processors to notify a personal data breach. The notification obligation lies with the controller.

☒       controller/ owner

This is usually a contractual requirement, as the processor processes data according to the controller's instructions, and an incident at the processor level that is notifiable according to the law needs to be notified by the data controller.

☐       data protection authorities
☐       cybersecurity authorities
☐       affected individuals
☐       others

# Sector-specific or Non-personal Data Security Breach Notification Requirements

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: January 2024*

Yes.

☐       public company obligations (e.g., to notify security incidents that may materially affect an investor's decision)

☐       cybersecurity authorities

☒      health regulatory requirements (e.g., to notify incidents affecting safety of medical devices)

☒       financial services requirements

☒       telecommunication requirements

☒       providers of critical infrastructure

☐        other

Some sector-specific regulations also provide notification obligations for companies subject to their regulatory framework.

BACEN's Regulation No. 4893 of 2021 imposes relevant requirements and specific obligations on financial institutions subject to BACEN's regulatory scope as regards the detection of incidents. Regarding the reporting of the data security breaches, the regulation requires the financial institution to report any security incidents that cause a "situation of crisis" to BACEN.

ANATEL's Regulation No. 740 of 2020, applicable to the telecommunications sector, establishes that the provider must notify ANATEL of relevant data security breaches that substantially affect the security of telecommunications networks and user data. There are further requirements on the required information that the notification must include.

ANEEL's Normative Instruction No. 964 of 2021, applicable to the energy industry, establishes that regulated agents must notify the designated sector coordination team of major data security breaches that substantially affect the security of facilities, operations or services. There are further requirements on minimum information that the notification must include.

# Cookies and Other Online Tracking Technologies

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last review date: January 2024*

ANPD has published general Guidelines on Cookies and Personal Data, clarifying a few uncertain points. The material was prepared with the purpose of guiding processing agents on good practices in the area, in addition to outlining an overview of the matter, addressing conceptual issues.

With an educational purpose, the Guidelines will be open to comments and continuous contributions from the public so that the material is always updated when new regulations are established.

Some of the changes introduced by these Guidelines include recommendations to:

Have a separate Cookie Policy in place (either as a separate document or as a separate section in the Privacy Policy)

Insert a specific checkbox in the Cookie Banner to reject non-strictly necessary cookies – this has to be made available in the first level banner, in a way that is easily seen by the user. This shall be an option in addition to the checkboxes.

Insert a link that is easily accessible in the first level Cookie Banner that would redirect the user to a general Privacy Policy, so that the data subjects can easily enforce their rights, and obtain more details about how their personal data are processed and for how long they are retained

Inform, in the second level Cookie Banner, how the user can block cookies on the browser settings and let the user know in case he/she will not be able to disable the cookies on the browser settings;

Present the Cookie Policy and Cookie Banner in Portuguese.

# Direct Marketing

## Are there specific requirements related to use of personal data for direct marketing activities?

*Last review date: January 2024*

Yes.

**☐        email marketing**

☐        prior opt-in consent
☐        opt-out or implied consent
☐        prior existing business relationship (and subject to other requirements) with opt-out consent

**☒         telephone marketing**

☐        prior opt-in consent
☒        opt-out or implied consent
☐        prior existing business relationship (and subject to other requirements) with opt-out consent

**☐         SMS/text message marketing**

☐        prior opt-in consent
☒       opt-out or implied consent
☐        prior existing business relationship (and subject to other requirements) with opt-out consent

**☐        postal marketing**

☐        prior opt-in consent
☐        opt-out or implied consent
☐        prior existing business relationship (and subject to other requirements) with opt-out consent

**☐        online behavioral advertising targeting/social media targeting/ad personalization marketing**

☐        prior opt-in consent
☐        opt-out or implied consent
☐        prior existing business relationship (and subject to other requirements) with opt-out consent

Brazil has very comprehensive consumer laws and regulations. Consumer authorities require consent from consumers whenever consumers are included in a marketing database. In July 2022, SENACON ordered several banking institutions to refrain from making any phone calls with the purpose of offering products/services without the consumers’ prior consent/existence of a database where the consumers’ data was lawfully obtained. According to such Authority, phone calls made with the purpose of offering products/services without previous consent are abusive and disturbing. Please note, though, that the consent referenced here is not the same consent under the LGPD for processing of personal data.

Although SENACON decisions are only applicable to B2C (business to consumer) relationships, please note that certain B2B relationships in Brazil may still be deemed a consumer relationship if the business is considered particularly vulnerable and is the end user of the service.

ANATEL has also issued regulations requiring the inclusion of the prefix 0303 in phone calls if they intend to offer new products and services.

# Accountability and Governance

## Are there accountability and governance requirements?

*Last review date: January 2024*

There are accountability and governance requirements to:

☒       take privacy by default and design measures for all processing of personal data
☒       perform and document data protection impact assessments (DPIAs) for high-risk processing:

There is no blacklist or whitelist as to what constitutes / does not constitute high-risk processing.

☒       maintain a record of processing activities
☒       implement appropriate measures to comply with data privacy and cybersecurity
☒       demonstrate compliance with data privacy and cybersecurity
☒       identify a specific individual as the data privacy contact for data subject or data protection authority inquiries
☒       provide training to employees
☒       audit or supervise data processors
☐       appoint a local representative in the jurisdiction (if the controller or processor is not located in the jurisdiction)
☐       other

# Penalties for Non-compliance

## What are the potential penalties / remedies for non-compliance with the key data privacy and cybersecurity laws in the jurisdiction?

*Last review date: January 2024*

There are:

☒       administrative remedies /civil penalties applied by regulators and law enforcement

According to the LGPD, sanctions include:

Warnings, with an indication of a deadline for correction measures to be undertaken

Simple fines of up to 2% of the net turnover of the economic group in Brazil, in its last fiscal year, limited to BRL 50 million (approx. USD 10.5 million) per violation

Daily fine, considering the total limits of the previous fine

Disclosure of the violation, after having properly verified and confirmed its occurrence

Blocking of the personal data the subject of the violation, until remedied

Deletion of the personal data, which is the subject of the violation

Suspension of the relevant database for six months, renewable for another six-month period

Suspension of the processing activities for six months, renewable for another six-month period

Prohibition of processing activities

Recently, the ANPD published the Regulation on the Calculation and Application of Administrative Sanctions, which establishes standards and criteria for the application of administrative sanctions by the Authority, as well as the forms and dosimetry for calculating the base value of fine sanctions.

☒       criminal penalties from regulators and law enforcement

According to the Brazilian Criminal Code, it is a criminal offense to invade third parties' information devices, whether or not such devices are connected to the internet, by means that aim to obtain, alter or destroy data or information without the express or implied authorization from the device owner or to install vulnerabilities to obtain illicit advantages. The crime is punishable by detention of three months to one year, plus a fine. This penalty also applies to anyone who makes, offers, distributes, sells or discloses a computer device or software aimed at enabling the conduct described above. Also, in the event that the invasion results in obtaining content from private electronic communications, industrial or trade secrets, confidential information or the unauthorized remote control of the device, the penalty is increased to imprisonment for six months to two years, plus a penalty. This latter penalty is also increased in the event that the data or information obtained is disclosed, traded or transmitted to third parties.

☒       private remedies

The imposition of administrative remedies does not preclude the right of affected individuals to claim indemnification for damages caused by the processing of personal data. The Brazilian Federal Constitution expressly entitles the data subject to indemnification for both moral and material damages for violations of the individual's rights to data protection, intimacy, privacy and honor.

☐       other

## If data subjects have private remedies, what form can these remedies take?

☒        individual personal actions

☒       representative actions (e.g., brought by a consumer / data privacy body or the supervisory authority)

☒       class actions

# Surveillance

## Are there separate laws or regulations regarding surveillance and/or technology which could be used for surveillance?

*Last review date: January 2024*

Yes.

If so, what is regulated:

☐        computer tracking / monitoring technology

☒        optical surveillance devices (e.g., CCTV cameras),

☐        audio surveillance / recording technology

☐        workplace surveillance

☐        facial recognition technology

☐        other biometric recognition technology

☐        other

Certain municipalities have specific municipal laws setting forth specific notices for optical surveillance devices.

# Risk Rating

## What is the risk of non-compliant data privacy and cybersecurity practices for private sector organizations in the jurisdiction?

*Last review date: January 2024*

☐       high(e.g., well-established privacy laws and regulations with strict compliance requirements, active regulator)
☒       medium(somewhere in between)
☐       low(e.g., relatively new or no privacy laws, inactive regulator)

# Most Common Compliance Mistakes

## What are the top three most common data privacy and cybersecurity compliance mistakes made by companies doing business in the jurisdiction?

*Last review date: January 2024*

☐        insufficient data subject notice

☒        lack of up-to-date record of processing

☒        insufficient data security or insufficient data security breach response

☒        insufficient agreements with processors

☐        lack of registration with /notification to / approval from the supervisory authority

☐        failure to address cross-border transfer requirements

☐        failure to address data residency requirements

☒        failure to appoint a data protection officer, local representative or similar position

☐        failure to comply with data subject rights requests

☒        lack of legal basis for processing (including invalid consent)

☐        lack of compliance with marketing requirements

☐        non-compliant automated decision making

☐        processing sensitive personal data incorrectly or without sufficient legal basis

☐        other

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: January 2024*

☐        Yes

☒        No

If yes, please provide a link

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: January 2024*

☐        Yes

☐        No

☒        It depends (for example, on the way the asset sale is structured, and/or the assets being acquired)

☐        Unclear

## If so, how would any regulatory fines be calculatedxx?

*Last review date: January 2024*

☐        Based on turnover of the entity (or group) that owned the assets at the time of the breach

☐        Based on the value of the transferred assets

☐        Based on the turnover of the entity (or group) that owned the assets at the time the breach is identified (which, if the breach is identified post-acquisition, may be the turnover of the acquiring entity or group)

☐        Based on the turnover of the entity (or group) that owned the assets at the time the fine is imposed (which, if the fine is imposed post-acquisition, may be the turnover of the acquiring entity or group)

☐        Based on a metric other than those outlined above

☒        Unclear

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: January 2024*

☒       Yes

☐       No

☐       It depends (for example, on the way the share sale is structured)

☐       Unclear

## If so, how would any regulatory fines be calculated?

*Last review date: January 2024*

☐        Based on the turnover of the target company (or its group) at the time of the breach

☐        Based on the turnover of the target company (or its group) at the time that the breach is identified (which, if the breach is identified post-acquisition, may be the turnover of the acquiring entity or group)

☐        Based on the turnover of the relevant entity (or group) at the time that the fine is imposed (which, if the breach is identified post-acquisition, may be the turnover of the acquiring entity or group)

☐        Based on a metric other than those outlined above#

☒        Unclear