Global Data and Cyber Handbook - Brazil

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

# What's new?

## Recently Updated Topics

This chapter is updated as of January 2025.

New sector-specific regulations have been published by the Central Bank (BACEN) and the National Council for the Rights of Children and Adolescents (CONANDA), which include relevant data privacy and cybersecurity obligations.

Further, the Brazilian Data Protection Authority (ANPD) published several relevant data protection documents in 2024. The ANPD also disclosed its Regulatory Agenda for 2025 and 2026, outlining the themes for which official regulations are expected to be issued soon.

# Key Data & Cyber Contacts

## Contacts



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

# Key Data & Cybersecurity Laws

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

*Last review date: 3 January 2025*

☒ 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: 3 January 2025*

[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 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)

It 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)

It 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 ANPD.

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. Key differences include lower monetary penalties, shorter timeframes to comply with data subject access requests, and a specific legal basis for credit protection.

## What are the key cybersecurity laws and regulations?

*Last review date: 3 January 2025*

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.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11200.htm)

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) **(as amended by Decrees** [**No. 9,832 of 2019**](https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9832.htm#:~:text=DECRETO%20N%C2%BA%209.832%2C%20DE%2012,que%20lhe%20confere%20o%20art.)**; No.** [**10,416 of 2020**](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Decreto/D10416.htm)**; No.** [**10,641 of 2021**](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10641.htm#:~:text=DECRETO%20N%C2%BA%2010.641%2C%20DE%202%20DE%20MAR%C3%87O%20DE%202021&amp;text=24%2C%20caput%20%2C%20inciso%20IX%2C,possam%20comprometer%20a%20seguran%C3%A7a%20nacional.)**; No.** [**10,849 of 2021**](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10849.htm#:~:text=DECRETO%20N%C2%BA%2010.849%2C%20DE%2028,Gestor%20da%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o.)**; No.** [**11,856 of 2023**](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.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.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10748.htm)

Published on 19 July 2021, this Decree establishes the Federal Cyber Incident Management Network. It is mandatory for offices and entities of the Federal Public Administration, while public companies and federal mixed-capital companies and their subsidiaries may participate voluntarily. The Decree aims to enhance coordination among Federal, Municipal, and State Public Administration entities in preventing, processing, and responding to cyber incidents, thereby improving the overall cybersecurity resilience of public entities.

[**Complementary Norm No. 08/IN01/DSIC/GSIPR**](https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=24/08/2010&amp;jornal=1&amp;pagina=1&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;jornal=1&amp;pagina=5&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 that 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/privacidade-e-seguranca/ppsi/guia_resposta_incidentes.pdf)

Published in December 2021 and updated in 2022, 2023 and 2024 (currently in version 3.3), this Guide provides good practices and guidelines for information security institutions and professionals to deal with cyber incidents, focusing on incidents involving personal data. It is applicable to professionals who are or will be assigned to the processing of personal data at 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 sets out the minimum information security requirements for the use of cloud computing solutions by bodies and entities of the Federal Public Administration. It applies to all Federal Public Administration bodies or entities that wish to use cloud computing. The regulation aims to ensure the safe use of cloud computing within the federal public administration.

[**Decree 11,491/2023**](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm)

Published on 12 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 cybercrime laws of member countries, facilitating their cooperation in criminal investigations and dialogue on cybercrime.

[**Decree 11,856/2023**](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm)

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.

**Resolution No. 245 of April 5, 2024**

On 9 April 2024, the National Council for the Rights of Children and Adolescents (CONANDA) published Resolution No. 245 of 5 April 2024, providing for the protection of children's and adolescent's rights in the digital environment. The resolution establishes principles and rights for the online protection of minors, including equality, freedom of expression, data security, and privacy. It also stipulates that only essential data should be collected, clear information about data processing must be provided, and where consent is the legal basis for processing, it should be free, collected before the processing, specific and highlighted. Companies are required to prevent minors from using services inappropriately, ensure they are held accountable for any abuses, implement age verification systems, and publish annual reports detailing transparency and risk management efforts.

**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 applies 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 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. It applies to all users and service providers of 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 for Information and Communication Technology (ICT) Solutions to be adopted by offices and entities within the direct and indirect administration of the executive branch of the State of Rio de Janeiro. Its purpose is to establish regulations 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 (ICT) Solutions to be observed by offices and entities within Rio de Janeiro's Public Administration. Its purpose is to establish regulations for these procedures and for the submission of requests to extend such contractual instruments 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 establishes the Information Security Policy for the Institute of Social Security of the State of Rio Grande do Sul ("**IPE Prev**"). It applies to users, managers, and outsourced contractors. The resolution aims to (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. 1 of August 12, 2020**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=1) **(as amended by Resolution** [**No. 30 of 2020**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=304)**,** [**No 39 of 2020**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=39)**,** [**No. 42 of 2020**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=42)**, No.** [**79 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=79)**, No.** [**88 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=88)**, No.** [**95 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=95)**, No** [**118 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=118)**, No.** [**103 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=103)**, No.** [**135 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=135)**, No.** [**147 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=147)**, No.** [**161 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=161)**, No.** [**167 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=167)**, No.** [**172 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=172)**, No.** [**176 of 2021**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=176)**, No.** [**181 of 2022**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=181)**, No.** [**269 of 2022**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=269)**, No.** [**293 of 2023**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=293)**, No.** [**342 of 2023**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=342)**, No.** [**402 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=402)**, No.** [**403 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=403)**, No.** [**425 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=425) **and No.** [**429 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=429)**)**

Published in 2020, this regulation establishes the Pix payment arrangement and approves its regulations. Developed by the Central Bank of Brazil, Pix is an instant payment system designed to facilitate real-time transfers and payments. The regulation includes security measures, including robust cybersecurity policies, incident response plans, and data processing protocols to be adopted by the companies that adhere to the Pix payment arrangement.

[**Open Finance - 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) **(as amended by Joint Resolution No. 3 of 2021, No. 4 of 2022 and No. 10 of 2024)**

Published in 2020, this regulation provides for the implementation of the Open Finance System. The Open Finance 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. Joint Resolution No. 10 of July 4, 2024 extended the criteria for mandatory participation in Open Finance for the purposes of data sharing and payment transaction initiation services.

[**National Monetary Council ("CMN") 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) **(as amended by** [**Resolution No. 5,117 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&amp;numero=5177)**)**

Published on 26 February 2021, this regulation provides for the cybersecurity policy and the requirements for contracting data processing, data storage and cloud computing services. It applies to institutions regulated by BACEN. 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) **(as amended by** [**BACEN’s Resolution No. 368/2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=368)**)**

Published on 8 April 2021, this regulation provides for cybersecurity policies and the requirements for contracting data processing, data storage and cloud computing services. It applies to payment institutions, securities brokerage firms, securities distribution firms, and foreign exchange brokerage firms authorized to operate by the BACEN. Its purpose is to ensure the confidentiality, integrity and availability of data and information systems used by such institutions.

[**Brazilian Securities and Exchange Commission Normative Ruling ("CVM") No. 35 of 2021**](https://conteudo.cvm.gov.br/legislacao/resolucoes/resol035.html) **(as amended by Normative Ruling** [**No. 134 of 2022**](https://conteudo.cvm.gov.br/legislacao/resolucoes/resol134.html) **and** [**179 of 2023**](https://conteudo.cvm.gov.br/legislacao/resolucoes/resol179.html)**)**

Published on 26 May 2021, this regulation is applicable to entities and individuals operating securities within the Brazilian stock market (intermediaries). Among other obligations, it requires intermediaries to (i) identify and list their relevant service providers; (ii) assess the controls performed by these service providers, and (iii) ensure that service agreements with these providers: (a) comply with the CVM’s requirement for intermediaries to maintain records of certain data for five years; (b) allow the regulated institution access to data and information processed or stored by the service provider; and (c) ensure the confidentiality, integrity, availability, and recovery of data and information processed or stored by the service provider.

[**BACEN's Resolution No. 304 of 2023**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=304)

Published on 20 March 2023, this regulation approves the requirements for the operation of settlement systems within the scope of the Brazilian Payment System, including the 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**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&amp;numero=6)

Published on 23 May 2023, the regulation sets out the 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 on profiles that indicate a greater propensity for risk in commercial transactions.

[**BACEN's Resolution No. 338 of 2023**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=338)

Published on 23 August 2023, the regulation 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 Resolution No. 342 of 2023**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&amp;numero=342)

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 non-compliance with Pix's technical security requirements.

[**BACEN's Resolution No. 412 of 2023**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&amp;numero=412)

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

[**BACEN’s Resolution 443 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&amp;numero=443)

Published on 12 December 2024, this resolution regulates the payment arrangement for "boletos" (payment slips), detailing their types, issuance, presentation methods, and the settlement of associated fund transfers. It outlines the obligations of participants in the payment slips system regarding data protection, requiring all participating institutions to implement comprehensive data protection measures to ensure the confidentiality, integrity, and availability of the data processed.

[**BACEN’s Normative Ruling No. 456 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&amp;numero=456) **(revoked by Normative Ruling No. 574 of 2024, effective as of July 1st, 2025)**

Published on 29 February 2024, this normative ruling introduced version 5.0 of the Open Finance Security Manual, which is binding for participants of the open finance system and contains detailed cybersecurity obligations. However, it was revoked by Normative Ruling No. 574 of 2024 and will cease to be effective as of 1 July 2025.

[**BACEN’s Normative Ruling No. 574 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&amp;numero=574)

Published on 20 December 2024, this Normative Ruling introduced version 6.0 of the Open Finance Security Manual, which is binding for participants of the open finance system and contains relevant and detailed cybersecurity obligations.

[**BACEN’s Normative Ruling No. 511 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&amp;numero=511) **(as amended by** [**Normative Ruling No. 581 of 2024**](https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&amp;numero=581)**)**

Published on 30 August 2024, this Normative Ruling regulates cybersecurity aspects for institutions participating in the Pix payment system. It requires the appointment of a director responsible for the institution's cybersecurity policy and requires the director to fill out a self-evaluation form on security.

**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 outlines the cybersecurity requirements for 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/13865)

Published on 19 March 2015, this resolution amends and consolidates the Information and Communications Security Policy of the Private Insurance Superintendence. The policy aims to establish strategic guidelines, responsibilities, and competencies to ensure the integrity, confidentiality, availability, and authenticity of the Private Insurance Superintendence's data and information, protecting 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 cybersecurity policies to be adopted by companies in the energy sector. Its purpose is to guarantee the security of information, technological infrastructure, and the privacy of customer 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, and amended by Resolution No. 767/2024, 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 cybersecurity 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 outlines the minimum cybersecurity requirements for establishing 5G networks. It applies to Federal Public Administration offices and entities responsible for implementing 5G networks. The ruling aims to enhance the protection of society and national institutions against potential vulnerabilities and backdoors in 5G technology systems.

[**ANATEL's Resolution No. 765/2023**](https://informacoes.anatel.gov.br/legislacao/resolucoes/2023/1900-resolucao-765)

Published on 6 November 2023, this resolution approves the General Regulation on Consumer Rights in Telecommunications Services. It grants consumers the right to information on measures applied by telecom providers to ensure the efficient and appropriate use of services, particularly regarding data management. Additionally, consumers have the right to privacy concerning 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 healthcare data of beneficiaries of a Private Health Care Plan. The TISS is a mandatory framework for the electronic exchange of healthcare data among private healthcare insurance providers not linked to the Brazilian Public Unified Health System (SUS). Its purpose is to promote interoperability between the health information systems of ANS and the Ministry of Health and to reduce information asymmetry for beneficiaries of private health care.

[**Administrative Resolution No. 81/2023 (ANS)**](https://bvsms.saude.gov.br/bvs/saudelegis/ans/2023/res0081_16_03_2023.html#:~:text=Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20de,o%20inciso%20II%20do%20art.)

Published on 13 March 2023, this resolution establishes the Information Security Policy for the National Health Agency (ANS). It outlines the objectives and guidelines for ensuring the confidentiality, integrity, and availability of information managed by ANS. The resolution includes several annexes detailing responsibilities and confidentiality agreements for various stakeholders, including employees, contractors, and external entities. It emphasizes the importance of protecting information assets, managing access permissions, and ensuring compliance with relevant legislation such as the LGPD. The policy applies to all ANS units and any individuals or entities interacting with ANS’s information and communication technology resources.

**Civil Aviation**

[**ANAC's Normative Ruling No. 128/2018**](https://www.anac.gov.br/assuntos/legislacao/legislacao-1/instrucoes-normativas/2018/instrucao-normativa-no-128-06-11-2018)

Published on 6 November 2018, and amended by normative ruling No. 173/2021, this regulation outlines ANAC's cybersecurity 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. 11126/2023**](https://pergamum.anac.gov.br/arquivos/PA2021-5805.PDF)

Published on 30 August 2021, and amended by ordinance No. 13990/2024, 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/aeroportos-e-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.

**Petroleum**

**National Agency of Petroleum, Natural Gas, and Biofuels (“ANP”) Ordinance 214/2023**

Published in February 2022, the Ordinance establishes the Information and Communications Security Policy for ANP. It outlines the guidelines to ensure the availability, integrity, confidentiality, and authenticity of ANP’s information. The policy applies to all ANP personnel, visitors, collaborators, and external agents accessing ANP’s environment, information assets, organizational processes, physical facilities, IT environments, and communication systems.

## What are the key laws and regulations relating to non-personal data?

*Last review date: 3 January 2025*

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

The Internet Legal Framework sets out principles, guarantees, rights, and duties for the use of the internet in Brazil. [It includes provisions on net neutrality, privacy, and data protection, and establishes guidelines for the storage and handling of internet data, which can include non-personal data](https://www.gov.br/mcom/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e-atividades/lei-geral-das-antenas).

[**Law 12,527/2011**](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm)

Also known as "Access to Information Law," the law regulates the procedures to be followed by public authorities to ensure access to information. [It mandates that public sector organizations disclose certain information of public interest, which can include non-personal data, to promote transparency and accountability](https://informacoes.anatel.gov.br/paineis/espectro-e-orbita/lei-das-antenas) among public authorities.

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

*Last review date: 3 January 2025*

Yes.

There are several Bills of Law aimed at amending the LGPD. They range from changes in the possible fines to be imposed in cases of misconduct to determining the criteria for allowing the use of personal data for training and improving artificial intelligence systems, among others. However, the most relevant regulations expected in the next 12 months are the new regulations to be issued by the ANPD.

Further, the AI Bill was approved by the Brazilian Senate. The AI Bill will now be sent to the House of Representatives for voting. 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, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 3 January 2025*

Brazil has a federal-level regulator for LGPD matters, the ANPD. Initially created as an entity associated with the Federal Presidency, it has been associated with the Ministry of Justice since January 2023 and has the authority to enforce the obligations provided under the LGPD and to apply statutory penalties, such as fines and even the 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 their respective data privacy and cybersecurity obligations, may result in enforcement against players of the industries subject to their regulatory framework.

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

*Last review date: 3 January 2025*

Consumer Authorities

☒ Very active

ANPD

☒ Moderately active

Sector-specific regulators

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

Consumer authorities are currently more active in enforcing data protection rights. While the ANPD is not as active yet, it has been increasing its enforcement efforts compared to previous years. This indicates a growing focus and commitment from the ANPD towards data protection regulation and compliance.

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

*Last review date: 3 January 2025*

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

Some of its key recent activities include the following:

The ANPD released the [Guide on Legitimate Interests](https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-guia-orientativo-sobre-legitimo-interesse), which [aims to clarify the application of legitimate interest as the legal basis for processing, ensuring transparency, predictability, and legal certainty in data processing activities](https://clym.io/data-privacy-news/anpd-brazil-publishes-guide-on-legitimate-interest-under-lgpd)

The ANPD published [Resolution CD/ANPD No. 15](https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024) ("Regulation on Notification of Security Incidents"). This regulation establishes mandatory procedures for data controllers to notify both the ANPD and data subjects about security incidents involving personal data, as required by the LGPD.

The ANPD released a [study on biometric data and facial recognition in Brazil](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/radar-tecnologico-biometria-anpd-1.pdf). The study aims to analyze the impacts, risks, and challenges associated with these technologies, particularly concerning the protection of personal data under the LGPD.

The ANPD published [Resolution CD/ANPD No. 18](https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074) ("Regulation on the Appointment of the Person in Charge"), which creates additional rules for the appointment of the Person in Charge.

The ANPD published [Resolution CD/ANPD No. 19](https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396) ("Regulation on International Data Transfer"), which details the data transfer procedure and provides the Standard Contractual Clauses (SCCs) for international data transfers.

The ANPD updated the [Data Protection Glossary](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd) and included new entries.

The ANPD published a translation of the LGPD and the Regulation on International Data Transfer.

The ANPD published the [Report on Generative AI](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/radar_tecnologico_ia_generativa_anpd.pdf), which aims to analyze the implications, risks, and challenges associated with generative AI technologies, particularly in the context of data protection under the LGPD.

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

The ANPD has published its Regulatory Agenda for 2025-2026, outlining its priority topics and expected dates for upcoming regulations. The agenda is divided into phases.

The ANPD expects to regulate data subject rights during the first phase, followed by Data Protection Impact Assessments (DPIAs), data sharing by government entities, minors' data processing, biometric data, security measures, artificial intelligence, high-risk processing of personal data, processing of personal data by religious organizations, and anonymization and pseudonymization.

In phase two, a national personal data protection and privacy policy, along with good practices and data governance rules, is expected to be prepared. Additionally, processing activities carried out by data aggregators will be regulated, with the aim of providing clear guidance on the transparency measures to be adopted, the appropriate legal basis for the processing of personal data and the limits on the use of data publicly available. The last topic planned to be regulated in phase two is health data.

Regulation on consent requirements is planned for phase three.

Finally, the regulation of the legal basis of credit protection is planned for phase four.

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 3 January 2025*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒         Increasing

Class actions/group actions under data or cyber regulation are:

☒         Increasing

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

*Last review date: 3 January 2025*

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 that is 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

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 ANPD, as well as the forms and the manner 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.

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

*Last review date: 3 January 2025*

☒        individual personal actions

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

☒       class actions

# Key Definitions

## Personal data

*Last review date: 3 January 2025*

The 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: 3 January 2025*

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

## Controller vs Processor

*Last review date: 3 January 2025*

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

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

The concept of "owner" and "agent" is not provided under the LGPD.

**Answer:** Yes

# Territorial Scope

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

*Last review date: 3 January 2025*

☒        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

☒        other

Applies to the processing of personal data collected in Brazil

# 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: 3 January 2025*

The following are potential legal bases for processing personal data:

☒        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 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 for processing 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 in legal, administrative or arbitral proceedings

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

The personal data is necessary for credit protection

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

*Last review date: 3 January 2025*

Yes

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 a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")

☒        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

☒        other

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

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

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

Compliance with legal or regulatory obligations 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.

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

*Last review date: 3 January 2025*

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 2023, the ANPD published a statement providing a standardized interpretation on the application of legal bases for the processing of children's and adolescents' personal data. According to the ANPD, the 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).

The Guide on Legitimate Interest, published in February 2024, contains a chapter dedicated to the use of legitimate interest in the processing of children's and adolescents' data. The ANPD recommended carrying out a balancing test, similar to the legitimate interest assessment, as a method to assess the existence of the best interests of the child and/or adolescent and to keep a record of the reasons for carrying out the processing.

## In what circumstances do these special requirements apply?

*Last review date: January 2025*

☒        generally

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

*Last review date: 3 January 2025*

☒       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. They must make information about the data categories collected, the use of such data, and the procedures to exercise data subject rights publicly available.

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

☒       other

Where consent is required, personal data relating to children may be collected without consent if it 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 a data subject's participation in games, internet applications, or 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 make every reasonable effort to verify whether the consent was given by the child's representative, considering the available technologies.

# Information Requirements, Data Subject Rights, Accountability and Governance

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

*Last review date: 3 January 2025*

☒        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 categories of personal data concerned

☒        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

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

☒        other

According to the [Regulation on the Appointment of the Person in Charge](https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074), it is necessary to disclose, in a prominent and easily accessible place (e.g., the website or other communication channels often used to contact data subjects), the name of the individual or legal person appointed as the person in charge, as well as their contact information). Therefore, although the LGPD does not expressly require companies to disclose the identity and contact details of the person in charge in the privacy notice to data subjects, this is the place where this information is usually disclosed.

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

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

*Last review date: 3 January 2025*

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

## Are there accountability and governance requirements?

*Last review date: 3 January 2025*

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

# DPOs and Notification Requirements

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

*Last review date: 3 January 2025*

There is the concept of a "person in charge," which is equivalent to a DPO under the GDPR (although not identical).

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

*Last review date: 3 January 2025*

☒        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. 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, self-employed, and non-profit associations. While not mandatory, an appointment of a person in charge will be considered good practice.

In 2024, the ANPD published the [Regulation on the Appointment of the Person in Charge](https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074), detailing the responsibilities of the person in charge. Such regulation establishes complementary rules on the appointment, definition and duties of the person in charge. It provides more details about the: (i) formal requirements on the appointment of the person in charge; (ii) personal attributes that the person in charge should meet; (iii) type of information about the person in charge's identity that must be publicly disclosed; (iv) the responsibilities and activities that the person in charge should perform; (v) cases where 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: 3 January 2025*

Yes

If yes, what are these requirements?

☒        other

The law requires that the identity and contact information of the person in charge be publicly disclosed, clearly and objectively, preferably on the company's website. In addition, the ANPD recommends that this information be also shared with the company’s employees.

Additionally, the [Regulation on the Appointment of the Person in Charge](https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074) stipulates that the appointment of the person in charge must take into account their professional qualities, particularly their knowledge of privacy and data protection matters. It further establishes that the person in charge can hold an additional role within the company or organization, provided it does not create a conflict of interest in the performance of their duties as the person in charge. Moreover, the person in charge must be able to communicate clearly and precisely with data subjects and the ANPD, in Portuguese.

## 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: 3 January 2025*

No.

# Data Processors

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

*Last review date: 3 January 2025*

Yes.

The obligations are as follows:

☒       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: 3 January 2025*

Yes.

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

# International Data Transfer

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

*Last review date: 3 January 2025*

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

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

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

On 23 August 2024, the ANPD published the [Regulation on International Data Transfer](https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396), which creates the procedures and rules for international transfers of personal data from Brazil to other countries. Companies have a 12-month deadline to ensure their transfers meet the requirements of the regulation (the deadline is in August 2025). Accordingly, the regulation sets out, among other aspects, the content of the standard contractual clauses as approved by the ANPD, and the manner by which data processing agents can otherwise ensure they have an adequate mechanism for international data transfers.

# Cookies, Online Tracking and Direct Marketing

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

*Last review date: 3 January 2025*

The ANPD has published general Guidelines on Cookies and Personal Data to clarify a few uncertain points. The material aims to guide processing agents on good practices in the area, providing an overview of the matter and addressing conceptual issues.

With a view to educating the public, the Guidelines will be open to comments and continuous contributions, ensuring 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 allow the rejection of 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 should 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 users know in case they are unable to disable the cookies on the browser settings

Present the cookie policy and cookie banner in Portuguese.

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

*Last review date: 3 January 2025*

Yes.

**☒  telephone marketing**

☒        opt-out or implied consent

**☒  SMS/text message marketing**

☒       opt-out or implied consent

Brazil has very comprehensive consumer laws and regulations. Such laws and regulations might require consent from consumers whenever consumers are included in a marketing database. Please note, though, that the consent referenced here is not the same consent under the LGPD for processing of personal data.

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.

# 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: 3 January 2025*

Yes.

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

It is the 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: 3 January 2025*

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

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.

## 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?

*Last review date: 3 January 2025*

No

The ANPD has issued two analyses and one proposal for an amendment of the AI Bill, which provides for the regulation of the use of artificial intelligence (AI) in Brazil. The ANPD has also published a public consultation for AI and the Automated Decisions Framework and a Report on Generative AI.

However, it has not mentioned anything specific about the use of artificial intelligence, automated decision-making or profiling in an employment context.

# 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: 3 January 2025*

Yes.

The restrictions or requirements are as follows:

☒       other

The data subject has the right to request the review of decisions taken solely based on the automated processing of personal data that 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: 3 January 2025*

Yes. Data controllers may refrain from complying with a request to review automated decisions to protect their trade secrets. But, in this case, the ANPD may audit the data controller to verify whether the automated decisions are discriminatory.

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

*Last review date: 3 January 2025*

No

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

In 2023, the ANPD published two preliminary studies on the AI Bill that aims to regulate the use of AI in Brazil. However, these studies are not binding and focus on the proposed AI Bill and the ANPD's role in 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).

In 2024, the ANPD submitted (i) proposals to amend the AI Bill; (ii) and opened a public consultation to regulate artificial intelligence and the review of automated decisions. Although it is still only a consultation, a possible future analysis of the contributions by the ANPD could lead to the drafting of more specific regulations on the subject in Brazil. The ANPD also published in 2024 a Report on Generative Artificial Intelligence that highlights some of the implications, risks and weaknesses of artificial intelligence systems related to the processing of personal data. However, as it is a research report, the study is not binding.

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: 3 January 2025*

☒         Enforcement activity against AI user(s)/deployer(s)

☒         Enforcement activity under existing privacy law

☒         Enforcement activity by data or cyber regulator

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

*Last review date: 3 January 2025*

☒       Draft legislation in progress

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

An AI Bill has been proposed before the House of Representatives. It aims to create rules for AI systems to be made available in Brazil, establishing the rights of those affected by their operation. It was already approved by the Brazilian Senate, but still needs to be sent to the Chamber of Deputies for analysis and approval. The Chamber of Deputies is entitled to make amendments to the AI Bill's current wording, before approval.

If the AI Bill is approved as per its current wording, people affected by artificial intelligence systems will have the right to challenge and request the review of decisions, recommendations or predictions generated by such a system that produce relevant legal effects or that significantly impact their interests. The AI Bill further defines the criteria for the use of these AI systems, including by the public authorities, providing for penalties for any violations of the law. It also provides the creation of an authority that will oversee and regulate this subject matter.

The AI Bill provides some criteria for companies to assess whether the AI system is considered as "excessive" or "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.

# 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: 3 January 2025*

No

## 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: 3 January 2025*

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

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

*Last review date: 3 January 2025*

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: 3 January 2025*

Yes

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

*Last review date: 3 January 2025*

Unclear

# Security Requirements and Breach Notification

## 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: 3 January 2025*

Yes.

☒        general obligation to take appropriate / reasonable technical, physical and/or organizational security measures  
☒        obligation to take specific security measures e.g., encryption  
☒       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 Regulation on Notification of Security Incidents, published on 26 April 2024, established the mandatory procedures that data controllers must follow when notifying security incidents to the ANPD and data subjects. The regulation provides that the notification must contain, among other information, the technical and security measures used to protect personal data, adopted before and after the incident, and the measures that have been or will be adopted to reverse or mitigate the effects of the incident on the data subjects.

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

*Last review date: 3 January 2025*

Yes.

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

Public companies in Brazil are required to maintain sufficient information security measures and ensure operational resilience to cyberattacks. The regulations include guidelines for the recording, collection and preservation of evidence of security incidents in Networks of offices and public entities, which are part of the Federal Public Administration.

☒       health regulatory requirements

Healthcare providers must implement security measures to protect patient data and ensure the integrity of health information systems.

☒       financial services requirements

Financial institutions are required to adopt cybersecurity policies and incident response plans to protect against cyber threats.

☒       telecommunication requirements

Providers must ensure the security and integrity of their networks, including measures to prevent unauthorized access and cyberattacks.

☒       providers of critical infrastructure

The regulations provide guidelines and instruments to safeguard critical infrastructure considered indispensable to national security. This includes integrating data on threats, security technologies and risk management.

☒       other

Insurance and Civil Aviation sectorial regulation

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

Please see responses above.

## 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?

*Last review date: 3 January 2025*

☒      Data privacy

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?"

In February 2024, the ANPD issued two penalties against Brazilian public bodies. In the first penalty, the ANPD imposed four warning sanctions on a federal public body for various breaches of the LGPD, including the failure to appoint a person in charge, the failure to send the data protection impact report requested by the authority and the failure to report a security incident that occurred in 2022. The second penalty was issued against another public body for failing to notify data subjects of a security incident involving personal data that occurred in 2022.

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

*Last review date: 3 January 2025*

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.

On 26 April 2024, the ANPD published the Regulation on Notification of Security Incidents.

The regulation provides 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 Regulation on Notification of Security Incidents sets forth parameters for when a security incident may give rise to relevant risk or damage to data subjects and, therefore, must be notified to the ANPD and the data subjects affected by that incident. It also sets forth the minimum information to be included in such a notification, and other relevant requirements regarding security incidents, such as the timeline for notification, the proceeding for notification before the ANPD, and the retention period for documentation related to the incident.

## Controllers/Owners have to notify:

*Last review date: 3 January 2025*

☒       data protection authorities

☒       affected individuals

Same as above.

## Processors/Agents have to notify:

*Last review date: 3 January 2025*

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.

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

*Last review date: 3 January 2025*

Yes.

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

☒      financial services requirements

☒      telecommunication requirements

☒      providers of critical infrastructure

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

For instance, BACEN's Regulation No. 4893 of 2021 imposes relevant requirements and specific obligations on financial institutions subject to BACEN's regulatory scope regarding the detection of incidents. In addition, 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 the minimum information that the notification must include.

# Data localization and regulation of non-personal data

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

*Last review date: 3 January 2025*

No generally speaking, except for a few specific sectoral regulations.

☒       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.

Also, there might be restrictions on the storage/transfer to foreign jurisdictions for certain types of information. For instance, according to CMN's Resolution no. 4,893/2021, which provides for requirements for the agreements between cloud providers and financial institutions, financial data does not necessarily need to be stored in Brazil, but the financial institution must ensure the access of the Brazilian Central Bank to the financial data. The access may be supported by the presence of a cooperation agreement between the Brazilian Central Bank and the supervisory authority from the jurisdiction where the data is stored. In case the data is stored in a jurisdiction where there is no such cooperation agreement, the agreement between the financial institution and the cloud provider must be submitted for the Brazilian Central Bank's approval.

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: 3 January 2025*

☒         Obligation for public sector organizations to share or make accessible non-personal data

Law No. 12,527/2011 (Brazilian Information Access Law) regulates access to public information held by government bodies. It aims to ensure transparency and accountability in public administration by providing citizens with the right to access information.

☒         Obligation for private organizations to share or make accessible non-personal financial data

BACEN and CVM Joint Resolution No. 6/2023 establishes the requirements that must be observed by financial institutions, payment institutions, and other entities authorized to operate by BACEN in the sharing of data and information on indications of fraud. The resolution mandates these institutions to share, through an electronic system, any data and information that support their fraud prevention procedures and controls. Institutions must obtain the prior and general consent of the customer to allow the registration and sharing of this data.

☒         Obligation for private organizations to share or make accessible other non-personal data

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

[Internet Legal Framework - Law No. 12,965/14](https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180) contains provisions regarding internet users' rights to the protection of logs, personal data and private communications. It includes, among others, obligations for internet application and connection providers to disclose internet access and connection logs upon receipt of a court order.

ANATEL’s Resolution No. 740/2020, amended by Resolution No. 767/2024, establishes guidelines and procedures to promote security in telecommunications networks and services, including the protection of critical infrastructures. The resolution requires telecommunications companies to retain and, in some cases, share certain types of data for regulatory and security purposes. This can include non-personal data related to network operations and usage.

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: January 2025*

Obligation to share data on request

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.