Global Data and Cyber Handbook - Brazil

Key Data & Cybersecurity Laws

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

# 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.

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.