Official Journal
of the European Union

EN
L series

2026/179

28.1.2026

COMMISSION IMPLEMENTING DECISION (EU) 2026/179

of 26 January 2026

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data by Brazil

(notified under document C(2026) 373)

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ([1]), and in particular Article 45 (3) thereof,

Whereas:

1. INTRODUCTION

(1) Regulation (EU) 2016/679 sets out the rules for the transfer of personal data from controllers or processors in the Union to third countries and international organisations to the extent that such transfers fall within its scope of application. The rules on international data transfers are laid down in Chapter V (Articles 44 to 50) of that Regulation. While the flow of personal data to and from countries outside the European Union is essential for the expansion of cross-border trade and international cooperation, the level of protection afforded to personal data in the Union must not be undermined by transfers to third countries ([2]).

(2) Pursuant to Article 45(3) of Regulation (EU) 2016/679, the Commission may decide, by means of an implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensure(s) an adequate level of protection. Under this condition, transfers of personal data to a third country may take place without the need to obtain any further authorisation, as provided for in Article 45(1) and recital 103 of Regulation (EU) 2016/679.

(3) As specified in Article 45(2) of Regulation (EU) 2016/679, the adoption of an adequacy decision has to be based on a comprehensive analysis of the third country's legal order, covering both the rules applicable to data importers and the limitations and safeguards as regards access to personal data by public authorities. In its assessment, the Commission has to determine whether the third country in question guarantees a level of protection 'essentially equivalent' to that ensured within the European Union ([3]). The standard against which the 'essential equivalence' is assessed is that set by European Union legislation, notably Regulation (EU) 2016/679, as well as the case law of the Court of Justice of the European Union ([4]). The European Data Protection Board's (EDPB) adequacy referential is also of significance in this regard to further clarify this standard and provide guidance ([5]).

([1]) OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Recital 101 of Regulation (EU) 2016/679.
([3]) Recital 104 of Regulation (EU) 2016/679.
([4]) Case C-311/18, Facebook Ireland and Schrems ('Schrems II') ECLI:EU:C:2020:559.
([5]) European Data Protection Board, Adequacy Referential, WP 254 rev. 01. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) As clarified by the Court of Justice of the European Union, a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order ([6]). In particular, the means to which the third country in question has recourse for protecting personal data may differ from the ones employed in the Union, as long as they prove, in practice, effective for ensuring an adequate level of protection ([7]). The adequacy standard therefore does not require a point-to-point replication of Union rules. Rather, the test lies in whether, through the substance of privacy rights and data protection safeguards (including their effective implementation, supervision, and enforcement), as well as through the circumstances surrounding a transfer of personal data, the foreign system as a whole delivers the required level of protection ([8]).

(5) The Commission has analysed the law and practice of the Federative Republic of Brazil ('Brazil'). Based on the findings set out in recitals (7) to (223), the Commission concludes that Brazil ensures an adequate level of protection for personal data transferred within the scope of Regulation (EU) 2016/679 from the European Union to Brazil.

(6) This Decision has the effect that transfers from controllers and processors in the Union to controllers and processors in Brazil may take place without the need to obtain any further authorisation. It does not affect the direct application of Regulation (EU) 2016/679 to such entities where the conditions regarding the territorial scope of that Regulation, laid down in its Article 3, are fulfilled.

2. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

2.1. The constitutional framework of Brazil

(7) Brazil is a Federative Republic composed of the union of the 26 States and the Federal District, as established in its Federal Constitution ('Constitution') ([9]). Brazilian States also have their own constitutions, which must not contradict the Federal Constitution ([10]). Brazil has a presidential system in which the President and members of the Legislative chambers (i.e. the Chamber of Deputies and the Federal Senate) are directly elected.

(8) Privacy and data protection are protected in the Constitution as fundamental rights. More specifically, Article 5 (X) of the Constitution protects intimacy and the private life of individuals, Article 5 (XII) guarantees the secrecy of correspondence communications, including data, and Article 5 (LXXIX) establishes the right to the protection of personal data online and offline ([11]).

(9) All rights under the Constitution apply to Brazilian and foreigners residing in Brazil pursuant to its Article 5. Federal laws have clarified that every person in the territory of Brazil, residing in it or not, is entitled to the protection of fundamental rights ([12]). The scope of the protection of such rights has been further extended by constitutional case law to encompass foreigners living abroad, as also highlighted by the relevant legal doctrine ([13]). As a result, any foreigner, resident or not in Brazil, can invoke these constitutional protections ([14]).

([6]) Case C-362/14, Schrems ('Schrems I'), ECLI:EU:C:2015:650, paragraph 73.
([7]) Schrems I, paragraph 74.
([8]) Schrems I, paragraph 75.
([9]) 1988 Constitution of the Federative Republic of Brazil. Available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.
([10]) Article 25, 1988 Constitution of the Federative Republic of Brazil.
([11]) Constitutional amendment N°115 of 10 February 2022. Available at: http://www.planalto.gov.br/ccivil_03/Constituicao/Emendas/Emc/emc115.htm#art1.
([12]) See for instance, Article 4 (XIII), Law N°13.445, of 24 May 2017, Migration Law. Available at https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm#:~:text=Institui%20a%20Lei%20de%20Migra%C3%A7%C3%A3o.&text=Art.,pol%C3%ADticas%20p%C3%BAblicas%20para%20o%20emigrante.
([13]) See e.g. FERREIRA FILHO, Manoel Gonçalves. Direitos humanos fundamentais. 6. ed. São Paulo: Saraiva, 2004.
([14]) Ruling from the Superior Tribunal de Justiça, 4a Turma, 2016. Available at: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.

(10) Brazil ratified the American Convention on Human Rights, known as the 'Pact of San José' in 1992 ([15]) ('Convention'). Among others, Article 11 of the Convention guarantees the right to privacy and Article 8 protects the right to a fair trial. In 1998, Brazil recognised the binding authority of the Inter-American Court of Human Right for the interpretation and application of the Convention ([16]). The Court can issue decisions concerning the application of rights in the context of activities conducted by public authorities in Brazil, including authorities carrying tasks for public security and defence purposes ([17]).

2.2. **The data protection framework in Brazil**

(11) Brazil has enacted in 2018 a general legislation in the area of data protection that provide safeguards for all individuals, irrespective of their nationality: the General Data Protection Law or 'Lei Geral de Proteção de Dados ('LGPD')' ([18]).

(12) Since its enactment, the LGPD has been strengthened and clarified through further legislation. In particular, the law N°13.853 of 2019 created Brazil's Data Protection Authority ([19]), called the Agência Nacional de Proteção de Dados, 'ANPD', which was made an independent authority through legislation adopted in 2022 ([20]). Further binding decrees supplemented these legislations, among others, to upgrade the status of the ANPD ([21]), further define its composition and the procedure to name its directors ([22]).

(13) As described in more detailed in recitals (125) to (141) of this Decision, the ANPD is the authority responsible for interpreting and enforcing the LGPD. In that context, it regularly issues binding regulations to interpret and apply the law. For instance, it has adopted several regulations to further develop the sanction regime and specify the rules on data breach notification ([23]). Further guidance on the application and interpretation of the LGPD is provided by the ANPD through documents and guides, such as the ones adopted on the interpretation of legal basis (e.g. legitimate interest) and of key concepts under the LGPD (e.g. sanctions, data protection officer).

([15]) List of signatories and ratification, American Convention on Human Rights. Available at: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm.

([16]) Declaration from Brazil regarding the Convention. Available at: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm#Brazil.

([17]) See, for instance, Case of Escher et al. v Brazil, Judgement of 6 July 2009. Available at: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf.

([18]) Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm and in English, at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf.

([19]) Law N° 13.853 of 8 July 2019 modifying the LGPD to, among others, create the data protection authority – Autoridade Nacional de Proteção de Dados (ANPD). Available at: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2.

([20]) Law N°14.460 of 25 October 2022 transforming the ANPD into an authority of special status. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7.

([21]) Decree N°1.317 of 17 September 2025 modifying the LGPD to transform the Agência Nacional de Proteção de Dados. Available at: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

([22]) Decree N°10.474 of 26 August 2020 establishing the ANPD and its composition. Available at: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Decree N° 11.758 of 30 October 2023 modifying the composition of the ANPD. Available at: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11758.htm. Decree of 5 November 2020 on the nomination of ANPD's directors. Available at: https://www.in.gov.br/en/web/dou/-/decretos-de-5-de-novembro-de-2020-286734594.

([23]) See list of Regulations of the ANPD. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes and in particular, Regulation N°4 of 24 February 2024 on the application of administrative sanctions. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077 and Regulation N°15 of 24 April 2024 on data breach notification. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.

(14) As part of its international engagement for the promotion and protection of data protection, Brazil's ANPD became a member of the Global Privacy Assembly in 2023, alongside all data protection authorities from the European Union ([24]). Brazil also joined, as observer, the Council of Europe's Committee on the Convention 108 for the protection of individuals with regard to automatic processing of personal data ([25]). Brazil has further been leading on several advancements made at the United Nations (UN) on the right to privacy. Alongside with Germany, Brazil introduced the United Nation Resolutions on the right to privacy in the digital age adopted by the UN General Assembly in 2013 and 2014 ([26]). Among other provisions, this Resolution notes that 'unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society'. It calls on states to review rules on data collections to align with international human rights law and to 'establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data' ([27]).

(15) In its structure and main components, Brazil's legal framework applying to the personal data transferred under this Decision is similar to the one applying in the European Union. This includes the fact that such framework does not only rely on obligations laid down in domestic law and rights guaranteed in its Constitution, but also on obligations enshrined in international law, in particular through Brazil's adherence to the American Convention on Human Rights and recognition of the jurisdiction of the Inter-American Court of Human Rights ([28]).

2.3. **Material and territorial scope of the LGPD**

2.3.1. *Territorial scope*

(16) The LGPD applies to any processing of personal data in Brazil regardless of the means used to carry out such activity ([29]).

(17) Article 3 of the LGPD specifies the territorial scope of the law indicating that it applies to: (1) processing activities carried out in the national territory of Brazil (which covers the Union, States, the Federal District and Municipalities); (2) processing activities that has the purpose of offering or supplying goods or services or the processing of data of individuals located in the national territory of Brazil; as well as (3) when the personal data processed have been collected in the national territory of Brazil. This is similar to the approach taken in Article 3 of Regulation (EU) 2016/679.

(18) In addition, pursuant to Article 3 (II) of the LGPD, all processing of personal data of natural persons who are in the national territory are covered by the law. This includes processing conducted for the monitoring of behaviour of individuals in the territory regardless of where the data is processed.

([24]) The Global Privacy Assembly (GPA) is a forum connecting the efforts of more than 130 data protection and privacy authorities from across the globe. See the ANPD's announcement when becoming a member of the GDA. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-aceita-como-membro-pleno-no-global-privacy-assembly.

([25]) Council of Europe, Observers to the Committee on the Convention 108. Available at: https://rm.coe.int/list-of-observers-december-2022-bilingual-2781-7012-1734-1/1680a962eb.

([26]) See, for instance, United Nations General Assembly, Resolution on the right to privacy in the digital age, 18 December 2013. Available at: https://digitallibrary.un.org/record/764407?ln=en&v=pdf.

([27]) United Nations General Assembly, Resolution on the right to privacy in the digital age, 18 December 2013, p. 1-2.

([28]) See Inter-American Court of Human Rights. Q&A on the jurisdiction of the Court. Available at: https://www.corteidh.or.cr/que_es_la_corte.cfm?lang=en.

([29]) Article 3, Law N°13.709 of 14 of August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

(19) Finally, according to the case law of the Federal Supreme Court (Supremo Tribunal Federal, 'STF'), it follows that the fundamental rights protections afforded under the Constitution, such as the right to data protection, apply to any person, regardless of the nationality or residency of the data subject ([30]).

2.3.2. *Definition of personal data*

(20) Article 5 (I) of the LGPD defines personal data as information related to an identified or identifiable natural person. The law specifies that a 'data subject' is a 'natural person to whom the personal data being processed refer' ([31]).

(21) In addition, pseudonymous information – i.e. information that can no longer directly or indirectly identify or be associated with a certain individual without using/combining additional information to restore the information to its original state – is considered personal data under the LGPD ([32]).

(22) Conversely, information that is fully 'anonymised' is excluded from the scope of application of the LGPD ([33]). Under Article 5 of the LGPD, anonymised data are defined as data that, through the use of reasonable and technical means available at the time of processing, cannot be directly or indirectly associated to an individual. Article 12 of the LGPD further details that anonymised data are not considered to be personal data except when the process of anonymisation to which the data were submitted has been reversed or if it can be reversed through 'reasonable efforts'. Article 12 of the LGPD also underlines that the determination of what is considered 'reasonable' shall take into account objective factors such as: (1) cost and time needed for the reversion; (2) the available technology; and (3) the exclusive use of a controller's own means. The approach to anonymisation and the safeguards introduced in the LGPD to address the possibility of re-identification is similar to the one followed in the EU.

(23) This corresponds to the material scope of Regulation (EU) 2016/679 and its notions of 'personal data', 'pseudonymisation', and 'anonymised information'.

2.3.3. *The definition of processing*

(24) The European Union and Brazilian systems' definitions of 'processing' both refer to 'any operation' carried out with personal data ([34]). Article 5 (X) of the LGPD provides for the following non-exhaustive list of activities that constitutes processing: 'collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, diffusion or extraction.'

2.3.4. *Controller and processor*

(25) The concept of data controller is defined in the LGPD as the natural or legal person, whether public or private, which is responsible for decisions concerning the processing of personal data ([35]).

([30]) Decision from the Superior Tribunal de Justiça, 4a Turma, 2016. Available at: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.
([31]) Article 5 (V), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([32]) Article 13, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([33]) Article 12, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([34]) Article 5 (X), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([35]) Article 5 (VI), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

(26) The concept of data processor is defined in the LGPD as the natural or legal person, whether public or private, which performs the processing of personal data on behalf of the controller ([36]). The processor must conduct the processing according to the instructions provided by the controller, who is responsible for verifying compliance ([37]).

(27) The controller and the processor must keep a record of the personal data processing operations they perform, especially when based on legitimate interest ([38]).

(28) Under the LGPD, two or more controllers who are directly involved in the processing from which the data subject has suffered damages are jointly and severally liable ([39]). A processor is jointly and severally liable for the damage caused by the processing when it fails to comply with the obligations of the LGPD, as defined under Article 44 of the LGPD, or when it has not followed the legal instructions of the controller ([40]).

(29) Therefore, the rules regulating the relationship between controllers and processors under the LGPD are similar to the ones under Chapter IV of Regulation (EU) 2016/679.

2.3.5. *Exemption from certain provisions of the LGPD*

(30) As in the European Union system, the LGPD does not apply to anonymised data ([41]), to processing of personal data for purely household purposes ([42]) or when conducted for the exclusive purposes of public safety, national defence, State security, or the investigation and prosecution of criminal offences ([43]).

(31) The exemption in the area of public safety, national defence, State security and the investigation and prosecution of criminal offences is however partial. The Federal Supreme Court has interpreted the applicability of the LGPD in light of the constitutional protection of personal data and established that the main principles, rights, and objectives of the LGPD apply to all processing of personal data by public authorities, including when conducted for 'intelligence' purposes ([44]). In addition, conditions for the processing of personal data for public safety, national defence, State security, or investigation and prosecution of criminal offences are set under Article 4 paragraphs 2 to 4 of the LGPD, in particular to prevent private entities to process data for such purposes, to instruct the ANPD to

([36]) Article 5 (VII), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([37]) Article 39, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([38]) Article 37, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([39]) Article 42, Paragraph 1, (II), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([40]) Article 42, Paragraph 1, (I), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([41]) Article 12, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([42]) Article 4 (I), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([43]) Article 4 (III), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([44]) Federal Supreme Court. Decision on ADI 6649, September 2022. Available at: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

issues technical opinions and recommendation on the matter, and to empower the ANPD to request data protection impact assessment in relation to these activities ([45]). On that basis, the ANPD has, for instance, conducted investigations and issued guidance, such as a technical note directed to the Ministry of Justice and Public Security regarding the use of technologies, including facial recognition, in public spaces ([46]). In this note, the ANPD recalled that processing for these purposes must comport with the general principles and rights provided by the LGPD ([47]).

(32) Article 4 (II) of the LGPD further introduces a partial exemption of the law for the processing of personal data for academic research purposes and for journalistic and artistic purposes.

(33) With respect to academic research, the exemption is limited by several elements. First, according to Article 4 (II) of the LGPD, the processing must be carried out 'exclusively' for academic research purposes. Second, Article 4 (II) (b) of the LGPD establishes that Articles 7 (requirement for legal basis) and 11 (rules on the processing of sensitive data) apply to these types of processing ([48]). Third, the ANPD has developed an orientation guide to further specify the rules applicable to the processing of data for academic and research purposes, including by strictly defining what entities can be considered a 'research body' as defined under Article 5 (XVII) of the LGPD ([49]). In this guidance, the ANPD confirms that the processing of data for academic research purposes is only partially exempted from the LGPD and that the general principles of the law will apply ([50]).

(34) Concerning specifically data used for health research, the LGPD contains additional limitations. On the one hand, Article 13 of the LGPD sets security obligations for databases used and encourages the use of anonymisation and pseudonymisation techniques. It also provides that research entities would be held liable for failure to implement security measure to protect the personal data ([51]). On the other hand, transfer of data used for health research to a third party 'is forbidden, under any circumstances' ([52]).

(35) With respect to the processing of personal data for journalistic and artistic purposes, the exemption of the LGPD is similar to the one provided for under Article 85(2) of Regulation (EU) 2016/679. The exemption under the LGPD covers situation where the processing would be done 'exclusively' for these purposes ([53]). This means, where press, media, and artistic bodies process personal data for other purposes, such as management of human resources or internal administration, the LGPD applies in full.

([45]) Article 4 paragraphs 2-4, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([46]) Technical Note N°175/2023 on the draft Cooperation Agreement between the Ministry of Justice and Public Security and the Brazilian Federation of Football for sharing personal data with a view to improving the 'Safe Stadium Project'. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

([47]) Technical Note N°175/2023, paragraph 5.1.

([48]) Article 4 (II) (b), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([49]) ANPD's Orientation Guide on the Processing of personal data for academic purposes and conducting research, June 2023. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf.

([50]) See, in particular, pages 18 to 43 of the Orientation Guide on the Processing of personal data for academic purposes and conducting research.

([51]) Article 13 Paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([52]) Article 13 Paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law. See also, ANPD's Orientation Guide on the Processing of personal data for academic purposes and conducting research, June 2023, p. 15.

([53]) Article 4 (II) (a), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

(36) Artistic expression and media freedom are both part of freedom of expression under Article 5 (IX) of the Constitution which guarantees the freedom of expression for 'intellectual, artistic, scientific and communication' speech. Concerning, the balancing exercise between freedom of expression and other rights (including the rights to privacy and data protection), it is governed by criteria set forth in the Constitution as interpreted by the Federal Supreme Court. In particular, the exercise of the right to freedom of expression does not require any prior authorisation, but it remains subjects to the limits imposed for the protection of other fundamental rights. Specifically, an individual may seek compensation in the event of harm or violation of the right to privacy, pursuant Article 5 (X) of the Constitution. Furthermore, these safeguards were integrated into the Civil Framework for the Internet, a law adopted in 2014 to protect fundamental rights online ([54]). In particular, Article 7 (I) of Civil Framework for Internet guarantees the 'inviolability of privacy' and establish a right to compensation for any material or moral damages resulting from a violation. Additionally, the STF refers in its case law about the need to 'establish a balance between rights, reconciling the right to free of expression with the inviolability of privacy', highlighting the importance of the right to redress and access to remedy in case of violation of privacy ([55]). In a different case, the STF recalled that 'the freedoms of the press and of social communication must be exercised in harmony with others constitutional principles' such as the inviolability of privacy and the right to data protection ([56]).

(37) Finally, the LGPD exempts from the scope of the law the processing of data that have their origin from outside of Brazil and are either (1) not shared or communicated to processing agents in Brazil; or (2) originating from a country that has been deemed adequate under the LGPD, as long as they are not transferred to another country ([57]). The ANPD has provided binding interpretation to clarify the two scenarios in a strict manner in its Data Transfer Regulation ([58]).

(38) Under the first scenario, the mere transit of personal data through Brazil, without any additional processing in the country, would be excluded from the law ([59]). However, as soon as data would be accessed, used, or otherwise processed in Brazil, the LGPD would apply. Existing domestic rules on cyber security and on access to data by public authorities would also continue to apply to this limited scenario, no matter whether the data is processed or stay in mere transit.

(39) In the second scenario, the ANPD has clarified that only the transfer back of data that has originally been transferred from a country benefiting from an adequacy decision under the LGPD is excluded from the law, as long as the national law of this adequate country would apply to that processing. In this case as well, the rules on cyber security and on access to data by public authorities would continue to apply. In the context of personal data being transferred between the EU and Brazil, in case the EU would benefit from an adequacy decision from Brazil, the transfer of data from Brazil back to the EU would not always fall under the scope of Article 3 of Regulation (EU) 2016/679. Therefore, in cases where the processing in questions would not fall within the scope of Regulation (EU) 2016/679, it results from Article 8 (II) (b) of the Data Transfer Regulation that the LGPD would apply to the transfer back of data from Brazil to the EU.

([54]) Law N°12.965 of 23 April 2014, Marco Civil da Internet ('Civil Framework for the Internet'). Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([55]) Federal Supreme Court, Decision on ADI 4815. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057.

([56]) Federal Supreme Court, Decision on ADI 5418. Available at: https://www.jurisprudencia.stf.jus.br/pages/search/sjur446943/false.

([57]) Article 4 (IV), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([58]) Section III, Annex I, ANPD, Regulation on International Transfer of Personal Data ('Data Transfer Regulation'). Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([59]) Article 8 (I), ANPD, Regulation on International Transfer of Personal Data.

2.4. **Safeguards, rights, and obligations**

2.4.1. *Lawfulness and fairness of processing*

(40) Personal data should be processed lawfully and fairly.

(41) The principles of lawfulness, good faith, and transparency and the grounds for lawful processing are guaranteed under Articles 6 and 7 of the LGPD through conditions that are similar to Articles 5 and 6 of Regulation (EU) 2016/679.

(42) Pursuant to Articles 6 and 7 of the LGPD, controllers and processors shall process personal information lawfully and in good faith to the minimum extent necessary for the specified purpose, covering data that are relevant, proportionate, and non-excessive in relation to the purpose ([60]).

(43) These general principles of lawful processing are further refined in Article 7 of the LGPD, which set out the different legal bases for processing including the circumstances under which this may involve a change of purpose.

(44) Pursuant to Article 7 of the LGPD, a controller and processor may only process personal data on a limited number of legal grounds. These legal grounds provided for under the LGPD are: (1) the consent of the data subject (lit. I); (2) the necessity to execute a contract or preliminary procedures related to a contract to which the data subject is party, at the request of the data subject (lit. V); (3) compliance with a legal or regulatory obligation by the controller ([61]) (lit. II); (4) to protect the life or physical safety of the data subject or a third party (lit. VII); (5) the processing of data by a public administration, that is necessary for the execution of public policies provided for in laws and regulations, or based on contracts, agreements or similar instruments ([62]) (lit. III); and (6) when necessary to fulfil the legitimate interests of the controller or a third party, except in case the fundamental rights and freedoms of the data subject that require the protection of personal data prevail (lit. IX).

(45) Article 7 of LGPD provides four additional specific legal bases for processing of data which are: (1) to carry out studies by research entities, ensuring, whenever possible, the anonymisation of personal data (lit. IV); (2) the regular exercise of rights in judicial, administrative or arbitration proceedings ([63]) (lit. VI); (3) for the protection of health, exclusively, in a procedure performed by health professionals, health services or health/sanitary authorities (lit. VIII); and (4) for credit protection (lit. X) ([64]).

([60]) See, in particular, Article 6, main paragraph, (III), (I), and (V) and Article 7, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([61]) Any legal or regulatory obligation shall be defined by law and be necessary and proportionate.

([62]) The specific provisions for the processing of personal data by public authorities provided for in Chapter IV of Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), shall be complied with.

([63]) The procedures are described in Law N°9.307 of 23 September 1996, Arbitration Law.

([64]) Regarding credit protection, the addition of this legal bases into the LGPD has increased the level of protection for data subjects by, for instance, ensuring that credit entities would only process the personal data necessary for credit analysis and recovery that is necessary. Since the adoption of the LGPD, Courts in Brazil have issued several decisions to, for instance, restrict the processing of data for credit protection purposes by excluding such as 'voter registration number, name of mother, lifestyle, social class, schooling, marginal propensity to consume and georeferencing' which were not deemed necessary. Courts have also clarified that further access to personal data would require the data subject's consent, therefore limiting the scope of data processing that can occur for credit protection. See, Opice Blum Advogados, Jurimetrics Report, 2022. Available at: https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf.

2.4.2. *Criteria for consent*

(46) The formal requirements for obtaining valid consent for processing personal data under the LGPD are set out in Article 8, following a similar approach to Articles 4(11) and 7 of Regulation (EU) 2016/679. First, consent must be given either in writing or through other means capable of demonstrating the data subject's 'manifestation of the will' ([65]). In its Guidelines, the ANPD has clarified that 'consent must be unequivocal, which requires obtaining a clear and positive expression of will from the data subject' which means that it is not permitted to obtain consent 'in a tacit manner or from an omission by the data subject' ([66]). Second, consent shall refer to 'particular purposes' and 'generic authorizations for processing' of personal data shall be considered void ([67]). Third, consent shall be informed through information provided in a 'transparent, clear and unambiguous' manner ([68]). When included within a broader contract, consent must appear in a distinct and specific clause that clearly stands out from the other contractual provisions ([69]). In addition, consent shall be considered invalid if the information provided to the data subject contains 'misleading or abusive content' ([70]). The controller must also inform the data subject of any changes regarding: (1) the specific purpose of the processing; (2) the type or duration of the processing; (3) the identity of the controller; or (4) any information regarding the processing and possible sharing of data ([71]). Fourth, consent can be 'revoked at any time' by the data subject through a 'free of charge procedure' ([72]).

(47) The LGPD establishes a strict prohibition on the processing of personal data where consent is defective or invalid ([73]). The LGPD further clarifies that the controller bears the burden of proof to demonstrate that consent was lawfully obtained in accordance with the LGPD ([74]).

(48) Finally, the LGPD establishes that in situation where consent would be the appropriate legal basis for processing, if personal data has been made 'manifestly public by the data subject', the requirement for consent is deemed waived ([75]). The concept of 'manifestly public data' is also found in Article 9 of Regulation (EU) 2016/679. However, even when consent is deemed waived, controllers and processors are not exempted from complying with all the other rights and obligations set out under the LGPD ([76]). In particular, data that has been made manifestly public by the data subject may be further processed provided that it is for a purpose that is 'legitimate and specific', and the rights of the data subjects and principles established under the LGPD are complied with ([77]).

([65]) Article 8 main paragraph, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([66]) ANPD, Guide on Cookies and Data Protection, p. 18-19. Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.

([67]) Article 8 paragraph 4, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law. In addition, where personal data is to be shared among controllers, a separate, specific consent is required for that sharing, unless the data was manifestly made public, as established by Article 7(5) of Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([68]) Article 9 paragraph 1, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([69]) Article 8 paragraph 1, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([70]) Article 9 paragraph 1, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([71]) Article 8 paragraph 6, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([72]) Article 8 paragraph 5, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([73]) Article 8 paragraph 3, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([74]) Article 8 paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([75]) Article 7 paragraph 4, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law. The scope of this measure is limited, as it does not cover the processing of sensitive data as authorised under Article 9(2)(e) of Regulation (EU) 2016/679.

([76]) Article 7 paragraph 4, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([77]) Article 7 paragraph 7, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

2.4.3. *Criteria for legitimate interest*

(49) Article 7 (IX) of the LGPD establishes that processing of personal data can never be carried out on legitimate interest grounds where such processing would conflict with the fundamental rights and freedoms of a data subjects, highlighting that the protection of personal data shall prevail. This approach is similar to one followed in the EU and set forth under Article 6(1)(f) of Regulation (EU) 2016/679.

(50) Article 10 of the LGPD sets out the additional conditions for controllers to rely on 'legitimate interest' as a legal basis for processing personal data. First, when processing of personal data is based on legitimate interest, the controller shall only process personal data which is 'strictly necessary' for the intended purpose ([78]). Second, controllers must also implement measures to ensure the transparency of their processing activities ([79]). Third, legitimate interest can only be relied on in 'particular situations' ([80]).

(51) Furthermore, the ANPD has published the 'Legitimate Interest Guide' which detailed the conditions for the use of the legitimate interest ([81]). This Guide, for instance, clarified that legitimate interest cannot be used a legal basis for the processing of sensitive data ([82]) and it also provides in its annex a model for the balancing test for the protection of fundamental rights and freedom that all controller seeking to rely on legitimate interest may use ([83]). Additionally, the ANPD may require the controller to conduct a data protection impact assessment ([84]).

(52) In the Guide, the ANPD clarified that for an interest to be considered 'legitimate', three conditions must be met: (1) compatibility with the Brazilian legal system; (2) reference to a specific situation; and (3) for the processing to be linked to legitimate, specific and explicit purposes ([85]). The first condition, 'compatibility with the legal system,' presupposes that the legitimate interest invoked by the controller must be compatible with the principles, legal standards, and fundamental rights guaranteed in Brazil. This means, for instance, that the envisaged processing of personal data should not be prohibited by a legislation in Brazil and cannot, directly or indirectly, contradict legal provisions or the principles found in Brazilian law. Second, the invoked legitimated interest must be based on 'concrete, clear and precise' situations, which aim at specific and well-defined interests. The invoked legitimate interest cannot be based on 'abstract or merely speculative situations' ([86]). The ANPD further specifies that interests that are not associated with the 'current activities of the controller are not considered legitimate' ([87]). The third condition refers to the need to demonstrate a specific purpose for processing. The ANPD notes that the legitimate interest of the controller (that justifies the processing) shall not be confused with the purpose of processing (which constitutes the specific purpose that is intended to be achieved by carrying out the processing). The existence of a

([78]) Article 10 paragraph 1, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([79]) Article 10 paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([80]) Article 10 of the LGPD provides some examples of the particular situations under which legitimate interest can be relied upon: (1) support and promotion of the controller's activities (lit. I); (2) protection the exercise of the data subject's rights, or to enable the provision of services that benefit the data subject, provided that such processing respects the data subject's legitimate expectations, fundamental rights, and freedoms (lit. II). Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([81]) ANPD, Guide – Legal bases for the processing of personal data – Legitimate Interest, February 2024 ('Legitimate Interest Guide'). Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf.

([82]) ANPD, Legitimate Interest Guide, p. 8.

([83]) ANPD, Legitimate Interest Guide, Annex 3.

([84]) Article 10 paragraph 3, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([85]) ANPD, Legitimate Interest Guide, p. 16-17.

([86]) ANPD, Legitimate Interest Guide, p. 16, interpreting Article 10 main paragraph of Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([87]) ANPD, Legitimate Interest Guide, p. 16.

legitimate interest does not eliminate the obligation for controller to comply with the principle of purpose limitation and all obligations under the LGPD. The purpose must be described clearly and precisely, with the information necessary to delimit the scope of the processing and enable the weighing of the interests of the controller or third parties with the rights and legitimate expectations of the data subjects ([88]). This means that when relying on legitimate interest for the purpose of supporting or promoting its activity, a controller shall, among other, clear define which activity it intends to promote/support and the link with the processing envisaged.

2.4.4. *Processing of special categories of data*

(53) Specific safeguards should exist where 'special categories' of data are being processed.

(54) Article 5 (II) of the LGPD defines sensitive personal data as 'personal data on racial or ethnic origin, religious conviction, political opinion, union affiliation or religious, philosophical or political organization, health or sexual life data, genetic or biometric data, when linked to a natural person.' As it resorts from the national case law, sexual life should be interpreted as also covering the individual's sexual orientation or preferences. In particular, in its case law on same-sex marriage, the STF ruled that discrimination based on 'sex' covers 'sexual preference' ([89]) and that the freedom to exercise one's 'sexual orientation' is a 'prerequisite for the development of one's personality', which is constitutionally protected ([90]). Therefore, the categories of data considered as sensitive data under Brazilian law are the same that under Article 9 (1) of Regulation (EU) 2016/679.

(55) The courts in Brazil have further expanded the definition of sensitive personal data under the LGPD to encompass other type of information that could be used to discriminate against individuals ([91]). This interpretation follows from the right to be protected against discrimination under Brazilian law, as also reflected in Article 6 (IX) of the LGPD. In particular, the Brazilian case law has clarified that information concerning criminal records shall be considered as sensitive data ([92]).

(56) The processing of sensitive data under the LGPD is only authorised when the data subject or his/her legal representative has given his/her 'specific and distinct' consent for specific purposes ([93]). The conditions for valid consent described in recitals (46) to (48) of this Decision apply.

(57) Pursuant to Article 11 (II) of the LGPD, without the explicit consent of the data subject, processing of sensitive data may be carried out: (1) when the processing is necessary for the compliance with a legal or regulatory obligation of the controller (lit. a); (2) when it is necessary for processing by public administration for the execution of public policies provided for in laws or regulations (lit. b); (3) to protect the life or physical safety of the data subject or a third party (lit. e); (4) for the exercise of rights, including in contract and in judicial administrative, and arbitration procedures, in accordance with Brazilian law (lit. d); (5) to protect the health of data subjects, exclusively in procedures carried out by health professionals, health services or sanitary authorities (lit. f); (6) by research entities to conduct studies, ensuring that data is anonymised, wherever possible (lit. c); and (7) to ensure the prevention of fraud and the safety of the data subjects, in processes of identification and authentication through registration in electronic systems. Therefore, the grounds for processing sensitive data under the LGPD and Regulation (EU) 2016/679 are similar.

([88]) ANPD, Legitimate Interest Guide, p. 17.

([89]) See ruling of Brazil's Federal Supreme Court authorising same-sex marriage, interpreting Article 3, section IV, of the Federal Constitution, which prohibits any discrimination based on sex, race, and color. Federal Supreme Court, Decision on ADI 4277 of 05 May 2011, points 2 and 6. Available at: https://portal.stf.jus.br/peticaoInicial/verPeticaoInicial.asp?base=ADI&numProcesso=4277.

([90]) See ruling of Brazil's Federal Supreme Court authorising same-sex marriage, p. 14: 'As an unshakable prerequisite for the development of human personality – the highest value protected by the Federal Constitution –, it is essential to remove any legal obstacle that represents a limitation – even a potential one – to the full exercise of the freedom that every human being has in the full exercise of their *sexual orientation'(emphasis added)*.

([91]) Superior Labour Court, Decision TST-E-RR-933-49.2012.5.10.0001, December 2021.Available at: https://www.jusbrasil.com.br/jurisprudencia/tst/713123452/inteiro-teor-713123472.

([92]) Superior Labour Court, Decision TST-E-RR-933-49.2012.5.10.0001, December 2021.

([93]) Article 11 (I), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

2.4.5. *Purpose limitation*

(58) Personal data should be collected for a specific purpose and in a manner that is not incompatible with the purpose of processing.

(59) Article 6 (I) of the LGPD establishes that personal data should be processed for a 'legitimate, specific, and explicit purpose of which the data subject is informed', with no possibility of further processing that is 'incompatible' with the original purpose. This principle, and its wording, is almost identical to the corresponding one in Article 5(1)(c) of Regulation (EU) 2016/679. Article 6 (II) of the LGPD further establishes that any processing activity must be compatible with the purposes communicated to the data subject.

(60) From guidance issued by the ANPD, it transpires that to determine whether processing for another purpose is compatible with the purpose for which data was initially collected, the controller shall demonstrate a link between the two processing purposes and take into account the 'legitimate expectations' of the data subjects ([94]). In case of processing for further compatible purposes, the principles and obligations of the LGPD shall apply, namely, to ensure that the new purpose is specific, and to guarantee the protection of data subjects' rights. This is also applicable to the further processing of data that has been made 'manifestly available' by the data subject or that is publicly available ([95]).

2.4.6. *Data accuracy and minimisation*

(61) Data should be accurate, and where necessary, kept up to date. It should also be adequate, relevant, and not excessive in relation to the purposes for which it is processed.

(62) These principles are guaranteed under the principles of 'quality of the data' and 'necessity' in Article 6 (III) and (V) of the LGPD, respectively. According to Article 6 (V) of the LGPD, the controller and processors shall ensure that personal data is accurate, clear, relevant, and up to date having regard to the purposes for which this data is processed. Article 6 (III) of the LGPD establishes the 'limitation of the processing to the minimum necessary' to achieve a specific purpose(s), 'covering data that are relevant, proportional and non-excessive' in relation to that purpose(s). These principles are similar to the ones set forth in Article 5(1)(c) and (d) of Regulation (EU) 2016/679.

2.4.7. *Storage limitation*

(63) Data should in principle be kept for no longer than is necessary for the purposes for which the personal data is processed.

(64) The principles of 'purpose', 'necessity', and 'access' set forth, respectively, in Article 6 (I), (III) and (IV) of the LGPD provides for requirements on storage limitation. They limit the possibility to store data to the minimum necessary in relation to a 'legitimate, specific and explicit' purpose and require data subjects to be informed about the duration of storage.

([94]) ANPD, Legitimate Interest Guide, p. 26 and Annex 2.

([95]) Article 7 paragraph 7, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law. See also recital (48) of this Decision. The concept of the data made 'manifestly available' is also found in Regulation (EU) 2016/679 while 'publicly available' data refer to information available in public registers or databases under Brazilian law pursuant to Law N°12.527 of 18 November 2011, Law on Access to Information. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

(65) In addition, Chapter II, Section IV of the LGPD is dedicated to the 'termination of data processing'. Under this Section, Article 16 of the LGPD requires that all personal data be deleted following the termination of processing for a defined purpose. These requirements, read in conjunction with the LGPD's principles of 'purpose', 'necessity' and 'access' are similar to the obligations deriving from Article 5(1)(e) of Regulation (EU) 2016/679.

(66) Pursuant to strict exceptions set forth under Article 16 of the LGPD, data may be further retained and stored: (1) for compliance with legal or regulatory obligations; (2) for research purposes, ensuring, whenever possible the anonymisation of the data; (3) when transferred to third parties in compliance with the LGPD's requirements; or (4) when used exclusively by the controller, as long as the data is anonymised and access to that data by third parties is prohibited.

(67) Data security requirement set forth under the LGPD and described in recitals (68) to (78) of this Decision apply to data kept in storage.

2.4.8. *Data security*

(68) Personal data should be processed in a manner that ensures their security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. To that end, operators should take appropriate technical or organisational measures to protect personal data from possible threats. These measures should be assessed taking into consideration the state of the art and related costs.

(69) This principle is guaranteed under Article 6 (VII) of the LGPD which mandates the use of 'technical and administrative measures' to protect personal data from 'unauthorised accesses and accidental or unlawful' processing, including 'destruction, loss, alteration, communication or dissemination' of data. To reduce these security risks, Article 6 (VIII) of the LGPD mandates the adoption of measures to 'prevent the occurrence of damages/harms due to the processing of personal data'.

(70) Article 44 of the LGPD establishes that the processing of personal data is unlawful when it fails to meet the security standards that a data subject is entitled to expect. The appropriate level of security must be determined, among others: (1) in light of the specific circumstances surrounding the processing carried out; (2) the reasonable level of risk expected; and (3) the techniques of processing available at the time it was carried out ([96]).

(71) To implement the data security principle, the LGPD set forth a series of requirement under Chapter VII, Section I on 'Security and Secrecy of Data'. Under this Section, Article 46 of the LGPD requires data controllers and processors to adopt 'security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful' processing, such as 'destruction, loss, alteration, communication or any type of improper or unlawful processing'. These measures shall be complied with 'from the conception phase of the product or service until its execution' ([97]). Article 47 of the LGPD imposes a general obligation on all parties involved in any phase of the processing to comply with the security requirements. These obligations are similar to the one set under Article 32 of Regulation (EU) 2016/679.

(72) Article 44 of the LGPD further establishes that the controller or processor who neglect to adopt security measures shall be held liable for damages causes in case of violation of security ([98]). The ANPD may also establish minimum technical security standards to ensure compliance with data security obligations ([99]).

([96]) Article 44 (I) to (III), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([97]) Article 46 paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([98]) Article 44 Sole paragraph, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([99]) Article 46 paragraph 1, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

(73) Pursuant to Article 48 of the LGPD, in the event of a security incident that may present a risk or cause significant harm to data subjects, the data controller is obliged to notify both the ANPD and the data subjects. Such notification must occur within a reasonable timeframe, as determined by the ANPD, and must include, at a minimum: (1) a description of the nature of the personal data affected; (2) information identifying the data subjects involved; (3) an indication of the technical and security measures employed to protect the data, subject to the preservation of commercial and industrial confidentiality; (4) an assessment of the risks associated with the incident; (5) an explanation for any delay in communication; and (6) a description of the measures taken or to be taken to mitigate or remedy the damage caused. The approach followed in the LGPD is largely similar to the one established by Articles 33 and 34 of Regulation (EU) 2016/679.

(74) The ANPD has adopted additional rules on data security incident to clarify, for instance, the definition of an 'incident' and the timeline for notification of an incident ([100]).

(75) Article 3 (XII) of Regulation on Security Incident Notification defines a security incident as 'any confirmed adverse event related to the violation of the confidentiality, integrity, availability and authenticity of personal data security'. Pursuant to Article 48 of the LGPD, a data breach and security incident that may create risks to data subjects must always be communicated to the data protection authority (ANPD) and the data subjects. Article 5 of the Regulation on Security Incident Notification clarifies that a security incident may entail a risk for data subjects when it may affect their interests and fundamental rights and if it involves at least one of the following type of data: (1) sensitive personal data; (2) data of children, adolescents or older people; (3) financial data; (4) authentication data in systems; (5) data protected by legal, judicial or professional secrecy; or (6) large-scale databases. In addition, a security incident will be considered as significantly affecting the fundamental interests and rights of data subjects, when: (1) it may prevent the exercise of rights or the use of a service; or (2) it may cause material or moral damages to the data subjects, such as discrimination, violation of physical integrity, the right to image and reputation, financial fraud or identity theft ([101]).

(76) Notification of a security incident to the ANPD and the data subjects shall take place within three working days of the controller becoming aware of it ([102]). The binding Regulation on Security Incident Notification clarifies to controllers the information that shall be provided to the ANPD and the data subjects. The data subjects' notification, in particular, shall include: (1) a description of the nature and category of personal data affected; (2) the technical and security measures used to protect the data; (3) the risks related to the incident, identifying the possible impacts on the data subjects; (4) the reasons for the delay, in the event that the communication was not made within 72 hours; (5) the measures that were or will be adopted to reverse or mitigate the effects of the incident, when applicable; (6) the date on which the security incident was discovered; and (7) the contact details for obtaining information and, when applicable, the contact details of the person in charge ([103]). When communicating the incident to the data subjects, controllers shall use 'simple and easy-to-understand language' ([104]). Notification shall be made directly and individually, if it is possible to identify the data subjects affected ([105]).

(77) In addition, the ANPD may, where necessary to safeguard the rights of the data subjects, evaluate the gravity of the incident and may instruct the controller to adopt specific measures ([106]). These may include the public disclosure of the incident through appropriate media channels, as well as the implementation of remedial or mitigating actions. A register of data security incident shall be kept by the data controller ([107]).

([100]) ANPD, Regulation on Security Incident Notification, April 2024. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.
([101]) Article 5 paragraph 1, ANPD, Regulation on Security Incident Notification, April 2024.
([102]) Articles 6 and 9, ANPD, Regulation on Security Incident Notification, April 2024.
([103]) Article 9 (I) to (VII), ANPD, Regulation on Security Incident Notification, April 2024.
([104]) Article 9 paragraph 1 (I), ANPD, Regulation on Security Incident Notification, April 2024.
([105]) Article 9 paragraph 1 (II), ANPD, Regulation on Security Incident Notification, April 2024.
([106]) Article 48 paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([107]) Article 10, ANPD, Regulation on Security Incident Notification, April 2024.

(78) Lastly, the LGPD links its standards of 'good practices and (data) governance' with the requirements on data security, in order to, among others, mitigate data processing risks ([108]). This includes promoting the adoption of internal privacy governance programmes to evaluate and mitigate risks ([109]).

2.4.9. *Transparency*

(79) Data subjects should be informed of the main features of the processing of their personal data.

(80) Following an approach comparable to Article 12 of Regulation (EU) 2016/679, Article 6 (VI) of the LGPD establishes that data subjects shall receive clear, precise, and easily accessible information about both the carrying out of their data processing and the respective processing agents, subject to 'commercial and industrial secrecy'.

(81) Article 9 of the LGPD establishes a list of information that shall be provided to the data subjects regarding the processing of data, which covers: (1) the specific purpose of the processing; (2) the type and duration of the processing; (3) the identification of the controller; (4) the controller's contact information; (5) information regarding the processing of data by the controller and the purpose; (6) the responsibilities of entities carrying out the processing; and (7) data subjects' rights, including information concerning the exercise of these rights.

(82) The limitation related to 'commercial and industrial secrecy' referred to in Article 6 (VI), and other provisions of the LGPD should be interpreted in light of Brazil's Law on Access to Information (LAI) ([110]). The LAI lays down as a rule the disclosure of information contained in registers or documents held by public bodies ([111]). Any exceptions – i.e. the imposition of restrictions on access to documents and information – must be justified and provided for by law ([112]). Commercial and industrial secrecy is one of those exceptions, with a specific legal provision to ensure the protection of 'information relating to the business activities of natural or legal persons governed by private law, obtained by other bodies or entities in the exercise of the activity of controlling, regulating and supervising economic activity, the disclosure of which could represent a competitive advantage for other economic agents' ([113]). The provisions of the LGPD referring to the 'commercial and industrial secrecy' shall therefore be interpreted in a manner that processing and otherwise disclosure of information shall not reveal business secret or create competitive advantage for other actors, while fulfilling the objectives of the protection of personal data. This means that, with respect to the principle of transparency, and throughout the text of the LGPD, the limitation for 'commercial and industrial secrecy' shall not be understood as a blanket ground for refusal for compliance with the law, but rather that specific safeguards shall be put in place to ensure disclosure of information in a way that protect these interests.

2.4.10. *Individual rights*

(83) Data subjects should have certain rights which can be enforced against the controller, in particular the right of access to data, the right to rectification, the right to have data erased, the right to object to processing, the right to portability and rights in the context of automated processing of data. These rights may be subject to restrictions, insofar as these restrictions are necessary and proportionate to safeguard specific objectives of general public interest.

([108]) Articles 49 and 50, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([109]) Article 50 main paragraph and paragraph 1, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([110]) Law N°12.527 of 18 November 2011, Law on Access to Information. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.
([111]) Articles 6 and 9, Law N°12.527 of 18 November 2011, Law on Access to Information.
([112]) Article 22, Law N°12.527 of 18 November 2011, Law on Access to Information.
([113]) Article 5 (2) of Decree No 7.721 of 16 May 2012, related to Law N°12.527 of 18 November 2011, Law on Access to Information.

(84) Chapter III of the LGPD establishes data subjects' rights in a similar way than under Articles 15 to 22 of Regulation (EU) 2016/679. The exercise of all rights is free of charge and data subjects must be informed of their rights ([114]). Pursuant to Article 21 of the LGPD, data concerning the exercise of rights by a data subjects cannot be used to her or his detriment. Data subjects may seek remedy in court, individually or collectively, in relation to their interests and rights ([115]).

(85) Data controllers shall 'immediately' inform data processors, with whom the data may have been shared, of data subjects' requests to rectification, erasure, anonymisation, restriction and objection to ensure that these requests can be complied with by all involved parties ([116]).

(86) Pursuant to Article 9 and Article 18 (II) of the LGPD, data subjects have a right to information and to access in order to obtain 'at any time', information regarding the processing of their data ([117]). This includes: (1) the identity of the controller (lit. III); (2) the controller's contact information (lit. IV); (3) information about the specific purpose of processing (lit. I); (4) information about the possible sharing of data (lit. V); (5) the type and duration of processing (lit. II); (6) the existence of data subjects' rights, including the right to lodge a complaint with the data protection authority; and (7) the responsibilities of the data processors. In addition, Article 10 paragraph 2 of the LGPD mandates the controller to be transparent about processing based on legitimate interest. Similarly, Article 9 of the Regulation on Data Transfers specifies that data subjects shall be informed in case of transfer of personal data.

(87) Article 19 of the LGPD further details the modality to provide data subjects with access to their personal information. Upon request from a data subject, access to personal data shall be provided: immediately, 'in a simplified format'; or within 15 days, by means of a clear and complete declaration ([118]). In addition, Article 19 paragraph 1 of the LGPD establishes that controllers shall store personal data in a format that facilitates the exercise of the right to access. Data subject may decide to receive their information by electronic form or on paper ([119]).

(88) Data subjects have the right to request the correction of incomplete, inaccurate, or out of date data, pursuant to Article 18 (III) of the LGPD (right to rectification).

(89) Article 18 (IV) and (VI) of the LGPD provides individuals with the right to request that their data be deleted, when: (1) it concerns unnecessary or excessive data; (2) for any data processed with the consent of the data subject; or (3) data is unlawfully processed. Furthermore, Section IV, Chapter II of the LGPD on the 'Termination of Data Processing' indicates that processing of data shall stop when a data subject either objects to the processing or withdraw its consent to the processing ([120]). Subsequently, data shall be deleted following the termination of processing ([121]). These provisions, read in conjunction, therefore indirectly expand the scope of the right to erasure under the LGPD.

([114]) Article 18, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([115]) Article 22, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([116]) Article 18 paragraph 6, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([117]) Article 6 (VI), Article 18, and Article 19, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([118]) Article 19 (I) and (II), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([119]) Article 19 paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([120]) See Article 15 (III), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), where 'communication by the data subject' refer, among others, to a revocation of consent (as indicated in the Article). The meaning of 'communication' is not limited to this scenario, and it allows data subjects to request a processing to stop.

([121]) Article 16, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

(90) Individuals have a right to oppose the processing of data based on legal basis other than consent, in case of non-compliance with the LGPD (right to object) ([122]). In addition, pursuant to Article 15 and Article 18 (IV) of the LGPD, data subjects have the right to restrict the processing of data ('blocking'). This right can be invoked, in particular, when the data processed is unnecessary or excessive, or when the data is processed in a manner that is non-compliant with the LGPD ([123]). Article 15 (II) of the LGPD indicates that data shall not longer be processed on the basis of a 'communication' from the data subject to the controller. Although this provision is subject to the 'public interest', interpreted broadly, provides for a wide scope for an indirect right to object in a way that is equivalent to the right to object provided for under Regulation (EU) 2016/679.

(91) Individuals have a right to request 'a complete electronic copy' of their data to allow for use by other entities (right to portability) ([124]). Similarly, as in the EU, data subjects may only request this copy when data have been processed on the basis of consent or a contract.

(92) Although any decision based on automated processing of data collected in the EU will typically be taken by a controller (who has a direct relationship with the concerned data subject and thus fall directly within the scope of Regulation (EU) 2016/679), it is worth nothing that the LGPD governs this type of processing in a way similar to Article 22 of Regulation (EU) 2016/679. First, Article 6 (IX) of the LGPD recognises the principle of non-discrimination as a data protection principle according to which it is prohibited to carry out processing of data for unlawful or abusive discriminatory purposes. This principle is applicable to all processing and is particularly relevant in context of automated processing. Then, pursuant to Article 20 of the LGPD, data subjects have the right to request the 'review of decisions made solely based on automated processing of data affecting his or her interests, including decisions intended to define his/her personal, professional, consumer and credit profile, or aspects of her/his personality'. When responding to a data subject request, controller must provide clear information about' the criteria and procedure used for automated decision' ([125]). In case such information cannot be provided to the data subject for reason of 'commercial and industrial secrecy' the ANPD has the power to carry out an audit to verify discriminatory aspects in automated processing of personal data ([126]). As a result, 'commercial and industrial secrecy' cannot be used a ground to refuse to address the request of the data subject.

(93) Article 23 of the LGPD states that specific legislations apply to the procedure and time period for exercising data subjects' rights when processed by public authorities ([127]). For instance, the Brazilian *Habeas Data* Law regulates the right to access to information for individuals regarding data held in registries or databases of the government or a public entity ([128]). The Brazilian *Habeas Data* Law establishes specific provisions for the right to access, which shall be granted within 10 days of an individual's request and a right to rectification, which shall be granted within 15 days of a request ([129]). Similarly, Brazil's Federal Administrative Procedure Law establishes a right to information and to access for individual in the context of administrative procedures ([130]). Brazil's Law on Access to Information

([122]) Article 18 paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([123]) Article 18 (IV), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([124]) Article 19 paragraph 3, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([125]) Article 20 paragraph 1, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([126]) Article 20 paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([127]) Article 23 paragraph 3, Law N°13.709 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([128]) Law N°9.507 of 12 November 1997, Brazilian Habeas Data Law. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm.
([129]) Articles 7 and 8, Law N°9.507 of 12 November 1997, Brazilian Habeas Data Law. The law provides for redress avenues in case of non-compliance with the individuals' request.
([130]) See, in particular, Article 6, Law N°9.784 of 29 January 1999, Federal Administrative Procedure Law. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. The law establishes procedures and timelines for communications with the individuals, as well as redress avenues in case of non-compliance.

also provides for obligations of information and transparency for public authorities, public companies, and the three branches of government (legislative, executive and judiciary) in Brazil ([131]). The provisions of these laws strengthen the right to access and to information established under the LGPD for the processing of data by public authorities. When these legislations do not provide for specific rights established under the LGPD (e.g. rights related to automated decision-making), data subjects may exercise these rights through the LGPD.

(94) Any violations of data subjects' rights will be treated by the ANPD as either a 'medium' or 'serious' infringement of the law, depending on the relevant factor and can therefore be subject to the highest level of sanctions and fines. Importantly, based on the ANPD's Regulation on Sanctions, the mere fact that a data subject right has been affected through a violation means that such an infringement cannot be considered as 'light' ([132]).

(95) Since the entry into application of the LGPD, the ANPD has been receiving a steady number of complaints and requests from individuals concerning their data protection rights ([133]). These numbers have increased significantly since July 2024, with the introduction by the ANPD of a modernised and easy to use platform for the submission of requests and complaints ([134]). Every month since, the ANPD receives around 400 complaints and 100 requests from individuals ([135]).

2.4.11. *Onward transfers*

(96) The level of protection afforded to personal data transferred from the Union to controllers and processors in Brazil must not be undermined by the further transfer of such data to recipients in a third country.

(97) Such 'onward transfers', constitute international transfers from Brazil from the perspective of the Brazilian controller.

(98) Chapter V of the LGPD establishes a framework for international transfers of personal data. The provisions under this Chapter are further complemented by a binding Regulation on international data transfers (Data Transfer Regulation) which was adopted by the ANPD in August 2024 ([136]).

(99) The Data Transfer Regulation defines a 'transfer' as 'processing operation through which a processing agent transmits, shares or provides access to personal data to another processing agent' and an 'international data transfer' as a 'transfer of personal data to a foreign country or to an international organization of which the country is a member' ([137]).

([131]) Article 1, Articles 6 and 9, Law N°12.527 of 18 November 2011, Law on Access to Information.

([132]) Article 8 paragraph 2, ANPD, Regulation on the calculation and application of administrative sanctions, February 2023 ('Regulation on Sanctions'). Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077.

([133]) ANPD, Report on the fourth year of the ANPD, November 2023, p. 24-25. Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view.

([134]) ANPD, Individual's platform. Available at: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados.

([135]) ANPD, Report on the fourth year of the ANPD, November 2023, p. 25.

([136]) ANPD, Regulation on International Data Transfers, August 2024. Available in Portuguese at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396 and in English, at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([137]) Article 3 (III) and (IV), ANPD, Regulation on International Data Transfers, August 2024 as well as Article 5 (XV), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

(100) The rules on international transfers established under the LGPD and the Data Transfer Regulation apply to all processing covered by the scope of LGPD. Article 7 of the Data Transfer Regulation expressly clarifies that the applicability of the LGPD to an international data transfer does not depend on the technical means used for processing, the geographic location of the data, or the physical presence of the controller or processor ([138]). Rather, what determines applicability is the existence of a substantive link between the data processing activity and Brazil.

(101) Similarly to Articles 44 to 49 of Regulation (EU) 2016/679, Article 33 of LGPD establishes the circumstances under which an international transfer of data can 'only' be allowed. These circumstances are further detailed in Article 9 of the Data Transfer Regulation.

(102) An international data transfer can take place if the following three, cumulative, circumstances are met: first, an international data transfer can 'only be carried out for legitimate, specific and explicit purposes informed to the data subject, with no possibility of onward processing incompatible with such purpose' ([139]). Second, the international data transfer must rely on a valid legal basis set forth under Article 7 of the LGPD (or Article 11 in case of sensitive data) ([140]). Third, a 'valid' data transfer mechanism must be used ([141]).

(103) Article 33 of the LGPD provides for several data transfer mechanisms.

(104) First, an adequacy decision can be adopted with respect to a third country or an international organisation (Article 33 (I)). In determining whether a third country or international organisation guarantees an adequate level of personal data protection, the ANPD shall consider several criteria set out under the LGPD and the Data Transfer Regulation ([142]) which are similar to the corresponding one under EU law. These include: (1) the general and sectoral legislation in force in the destination country or applicable to the international organisation, that have a direct impact on the protection of personal data ([143]); (2) the nature of the data ([144]); (3) ensuring that the third country or international organisation provides for a level the protection of personal data and guarantees the rights of data subjects that is consistent with the LGPD ([145]); (4) the adoption of appropriate technical and organisational measures to ensure data security and to mitigate the risks of adverse impacts on privacy and other fundamental rights ([146]); (5) the existence of judicial and institutional mechanisms to guarantee data protection rights, in particular through the existence of an independent supervisory authority with adequate powers and resources to monitor and enforce data protection provisions ([147]); and (6) any other specific circumstances relevant to the context of international data transfer ([148]).

([138]) Article 7, ANPD, Regulation on International Data Transfers, August 2024.
([139]) Article 9, ANPD, Regulation on International Data Transfers, August 2024.
([140]) Article 9 (I), ANPD, Regulation on International Data Transfers, August 2024.
([141]) Article 9 (II), ANPD, Regulation on International Data Transfers, August 2024.
([142]) Article 34, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) and Chapter V, ANPD, Regulation on International Data Transfers, August 2024.
([143]) Article 34 (I), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) and Article 11 (I), ANPD, Regulation on International Data Transfers, August 2024.
([144]) Article 34 (II), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) and Article 11 (II), ANPD, Regulation on International Data Transfers, August 2024.
([145]) Article 34 (III), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) and Article 11 (III), ANPD, Regulation on International Data Transfers, August 2024.
([146]) Article 34 (IV), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) and Article 11 (IV), ANPD, Regulation on International Data Transfers, August 2024.
([147]) Article 11, paragraph 3, ANPD, Regulation on International Data Transfers, August 2024.
([148]) Article 34 (VI), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) and Article 11 (VI), ANPD, Regulation on International Data Transfers, August 2024.

(105) For the evaluation of the level of protection of personal data in the context of an adequacy decision, the ANPD will also assess: (1) the risks and benefits provided by a specific adequacy decision, considering, among other aspects, the guarantee of the principles, the rights of the data subject, and the data protection regime provided for the LGPD; as well as (2) the impacts of the decision on the international flow of data, diplomatic relations, international trade, and Brazil's international cooperation with other countries and international organisations ([149]). The assessment and issuance of an adequacy decision is under the responsibility of the ANPD ([150]). Currently, the ANPD is only working on an adequacy decision with the European Union.

(106) Second, Article 33 (II) establishes that data transfers may take place when controllers ensure 'guarantees of compliance with the principles and rights of the data subjects and the regime of data protection' provided by the LGPD. This can be guaranteed through (1) specific contractual clauses (point II, lit. a); (2) standard contractual clauses (point II, lit. b); (3) binding corporate rules (point II, lit. c); or (4) approved seals, certification, and codes of conducts (point II, lit. d).

(107) Controllers may rely on specific contractual provisions for international transfer as well as on standard contractual clauses approved by the ANPD ([151]). Under the Data Transfer Regulation, the ANPD has adopted a set of model contractual clauses that cover all relevant data protection requirements (i.e. data subjects' rights, independent oversight and supervision, data security measures, safeguards on onward transfers, etc.) ([152]). These clauses include provisions that cannot be changed by the parties to the contract ([153]). The clauses are modular to adapt to different data transfer scenarios (e.g. controller to processor, processor to processor) ([154]).

(108) Concerning Binding Corporate Rules (BCR), the ANPD clarifies in Chapter VI of the Data Transfer Regulation how this mechanism can be used, as well as the requirements of their validity. The ANPD recalls, in particular the 'binding nature' of the instrument on all 'members of the group or conglomerate' that rely on it, requirements concerning data subjects' rights and their exercise, the applicable liability and responsibility rules ([155]), and all mandatory information that a BCR shall include ([156]). BCR are subjects to the prior approval of the ANPD pursuant to a process defined in Chapter VIII of the Data Transfer Regulation which require companies to submit complete documentation to the ANPD and involve a review process from the ANPD ([157]). Companies are also required to communicate with the ANPD any issues that may affect compliance with the LGPD, including when members of the group become subject to foreign obligations ([158]). All approved BCRs will be published on the webpage of the ANPD, and companies have the obligation to transparently inform about the international transfer carried out ([159]).

([149]) Article 12, ANPD, Regulation on International Data Transfers, August 2024.

([150]) The procedure for issuance of an adequacy decision is described under Section III, Regulation on International Data Transfers, August 2024.

([151]) Article 35, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([152]) Annex II, ANPD, Regulation on International Data Transfers, August 2024.

([153]) Annex II, Section II, ANPD, Regulation on International Data Transfers, August 2024.

([154]) Annex II, Clause 4, ANPD, Regulation on International Data Transfers, August 2024. Controllers and processors may choose the appropriate 'option' corresponding to their circumstances under this clause.

([155]) Article 3 (VIII), ANPD, Regulation on International Data Transfers, August 2024. The definition of 'responsible entity' establishes that a 'business company, headquartered in Brazil, is liable for any breach of a binding corporate rule, even if resulting from an act by a member of the economic group headquartered in another country', following a similar approach than Article 47(1)(f) of Regulation (EU) 2016/679.

([156]) Article 27, ANPD, Regulation on International Data Transfers, August 2024.

([157]) Articles 27, 28 and Chapter VIII, ANPD, Regulation on International Data Transfers, August 2024.

([158]) Article 25 (VIII), ANPD, Regulation on International Data Transfers, August 2024.

([159]) Article 32, ANPD, Regulation on International Data Transfers, August 2024. This article further indicates that companies have the obligation to make the BCRs available to data subjects upon request.

(109) The ANPD may also designate certification entities to develop seals, certification, or codes of conducts for data transfers ([160]). The decisions and activities carried out by these certifications' entities may be reviewed by the ANPD, who can review and revoked decisions, in case of non-compliance with the LGPD ([161]).

(110) Finally, the LGPD provides a list of 'specific situations' under which an international transfer may be carried out when: (1) necessary for international legal cooperation between public agencies, in accordance with international law; (2) necessary to protect the life or physical safety of the data subject or a third party; (3) authorised by the ANPD; (4) related to a commitment under international cooperation; (5) necessary for the execution of a public policy or legal obligation of a public authority; (6) data subjects has consented to the specific transfer of data, with prior information of the nature of the processing; or (7) when necessary for compliance with a legal or regulatory obligation, in relation to the provision of a contract, or for the exercises of rights in judicial, administrative or arbitration procedures ([162]). As indicated in the Data Transfer Regulation, international transfers can only be carried out under these scenarios if 'the specificities of the particular case and the applicable legal requirements are met' ([163]).

(111) Concerning the specific situation under which data transfer can be carried out on the basis of data subjects consent, it requires that (1) the formal criteria for obtaining valid consent are met (i.e. be specific, freely given, explicit, informed); (2) data subjects are informed of the nature of the transfer *before* it is carried out (e.g. information about the jurisdiction of the intended transfer and the level of protection it guarantees; information about the absence of an adequacy decision or of other data transfer mechanisms; information about the duration of the transfers); and (3) consent must be obtained for each transfer specifically and separately from any other processing. As indicated in recital (46), tacit agreement cannot be considered as valid consent and data subjects have the right to withdraw consent at any time.

(112) The Data Transfer Regulation strictly frames the uses of all these mechanisms on the basis of several conditions. This includes, in particular, providing 'clear, accurate and easily accessible information on the transfer' to the data subject, as well as guaranteeing and being able to demonstrate that the international transfers are carried out in a manner that ensure the compliance with the principles and the rights of the data subject, and does not alter the level of protection provided in the LGPD, 'regardless of the country where the personal data subjected to the transfer is located, even after the end of the processing and in the cases of onward transfers' ([164]). These requirements also apply when conducting transfers on the basis of 'specific situations', to ensure a continuity of protection regardless of the instrument used to carry out an international transfer.

(113) The rules described in recitals (96) to (112) of this Decision therefore ensure continuity of protection when personal data is onward transferred from Brazil in a way that is essentially equivalent to what is provided under Regulation (EU) 2016/679.

2.4.12. *Accountability*

(114) Under the accountability principle, entities processing data are required to put in place appropriate technical and organisational measures to effectively comply with their data protection obligations and be able to demonstrate such compliance, in particular to the competent supervisory authority.

([160]) Article 35, paragraph 3, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([161]) Article 35, paragraph 4, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([162]) Article 33 (III) to (IX), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([163]) Article 1 (Sole paragraph), ANPD, Regulation on International Data Transfers, August 2024.

([164]) Article 2 (I) and (IV) and Article 4, ANPD, Regulation on International Data Transfers, August 2024. As all international transfers, any transfer carried out under these scenarios shall be for 'legitimate, specific, and explicit purposes informed to the data subject, with no possibility of onward processing incompatible with such purposes' as established by Article 9, main paragraph, ANPD, Regulation on International Data Transfers, August 2024.

(115) Article 6 (IX) of the LGPD establishes the principle of accountability according to which the controller and processor shall adopt measures which are 'efficient and capable' of demonstrating compliance with the LGPD.

(116) As a means to ensure accountability, Article 50 of the LGPD provides that controllers and processors may adopt internal rules and governance models, in particular to ensure good practices in handling complaints and petitions from data subjects, observing security obligations and all other obligations under the LGPD ('Good practices and governance'). These programmes should also include plans for educational activities, internal supervision mechanism and risk mitigation.

(117) The LGPD also provides a requirement to appoint a data protection officer (DPO) which has a significant role in the design and implementation of these internal programmes. Pursuant to Article 5 (VIII), the DPO shall serve as a link between the controller, data subjects and the ANPD. Article 41 of the LGPD mandates all controllers to appoint a DPO and for his or her identity to be publicly disclosed.

(118) The LGPD has empowered the ANPD to introduce exemption to the obligation for controllers and processors to appoint a DPO ([165]). In its Regulation on the application of the LGPD to Small and Medium Enterprises (SMEs), the ANPD established that certain small companies, SMEs, start-ups, and non-for-profit organisations may fall under this exemption ([166]). Specifically, the scope of the exemption covers the following entities: 'micro-enterprises, small businesses, startups, legal entities under private law, including non-profit organisations, in accordance with current legislation, as well as natural persons and depersonalised private entities that process personal data' ([167]). Under Brazilian law, microenterprises ([168]), small business ([169]), or start-up ([170]) refer to companies with a sole or a low number of employees ([171]), and that fall below a certain yearly gross revenue ([172]).

(119) The exemption to appoint a DPO would not apply to any of these companies and entities, no matter their size or revenues, which carries out a 'high-risk' processing of personal data ([173]). A processing will be considered high-risk, if it, cumulatively, falls in, at least one of these general characteristics: (1) processing of personal data on a large scale; and (2) processing of data that may significantly impact the fundamental rights and interests of the data subjects; and at least one of these specific characteristics: (1) use of emerging or innovative technology; (2) surveillance or control of areas accessible to the public; (3) solely automated decision-making processes; and (4) processing of sensitive data or data belonging to children or older people ([174]). A 'large-scale' processing of personal

([165]) Article 41, paragraph 3, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([166]) ANPD, Regulation on the application of the LGPD to Small and Medium Enterprises ('Regulation on SMEs', April 2024. Available at: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022.

([167]) Article 2 (I), ANPD, Regulation on SMEs, April 2024.

([168]) A 'micro-enterprise' is defined as a company with a yearly gross revenue equal to or below Brazilian Reals ('R$') 360 000. See, Article 3 (I), Complementing Law N°123 of 14 December 2006, Law on the National status of micro, small and medium companies. R$ 360 000 is the equivalent of EUR 56 500.

([169]) A 'small business' or 'SME' is defined as a company with a yearly gross revenue of at least R$ 360 000 and equal or inferior to R$ 4 800 000. See, Article 3 (II), Complementing Law N°123 of 14 December 2006, Law on the National status of micro, small and medium companies. R$ 4 800 000 is the equivalent of EUR 753 000.

([170]) A 'start-up' is defined as a 'business or corporate organisations, whether nascent or recently operating, whose activities are characterised by innovation applied to the business model or products or services offered'. See, Article 2 (III), ANPD, Regulation on SMEs, April 2024.
A start-up can only be registered as such for a maximum of 10 years and with a yearly gross revenue limited at R$ 16 000 000. See, Article 4 (I), Complementing Law N° 182 of 1 June 2021, Law on start-ups. Available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp182.htm. R$ 16 000 000 is the equivalent of EUR 2 500 000.

([171]) See, in particular, Article 2 (II), ANPD, Regulation on SMEs, April 2024 and Article 41, Law N°14.195 of 26 August 2021, Law on the opening of companies. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14195.htm.

([172]) Complementing Law N°123 of 14 December 2006, Law on the National status of micro, small and medium companies. Available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm.

([173]) Article 4, ANPD, Regulation on SMEs, April 2024.

([174]) Article 4 (I) and (II), ANPD, Regulation on SMEs, April 2024.

is defined as a processing that 'involves a significant number of data subjects, also considering the volume of data involved, as well as the duration, frequency and geographic extent of the processing carried out' ([175]). A 'processing of data that may significantly impact the fundamental rights and interests of the data subjects' is defined 'among other situations, those in which the processing activity may impede the exercise of rights or the use of a service, as well as cause material or moral damages to the data subjects, such as discrimination, violation of physical integrity, the right to image and reputation, financial fraud or identity theft' ([176]).

(120) The ANPD adopted a binding Regulation on the role of the DPO which further clarifies its duties ([177]). In this Regulation, the ANPD recalls the obligations for private entities and public authorities to publish information on the identity of their DPO ([178]). Article 10 of the DPO Regulation recalls the obligation for controllers and processors to, among others, ensure that the DPO can carry out its tasks with independence, 'free from undue interference, especially in providing guidance on the practices to be adopted in relation to the protection of personal data' and that the DPO is given direct access to the highest management level and all employees involved in strategic decisions for the processing of data within an entity. Similarly, the DPO shall carry out its duties and tasks with 'ethics, integrity and technical independence, avoiding situations that may constitute a conflict of interest' ([179]).

(121) The role of the DPO has been a priority of the ANPD's enforcement action. For instance, the ANPD's first ever sanctions concerned a company, which was fined and received a specific warning for falling to demonstrate its had appointed a DPO ([180]). The entity resolved to appoint a DPO during the administrative proceeding to comply with the ANPD's order. Since then, the ANPD has continued issuing sanctions to public and private entities in relation to the DPO provisions established under the LGPD ([181]).

(122) Data Protection Impact Assessment (DPIA) are another important tool to ensure accountability. DPIA allow to assess and determine the impact of a processing. According to Article 38 of the LGPD, the ANPD can request a controller or processor to establish a DPIA ([182]), which must include a description of the type of processing of the personal data as well as measures, safeguards, and mechanisms to mitigate risks. In addition, Section II of LGPD establishes provisions on accountability which empowers the ANPD to request the publication of DPIA or recommend the adoption of 'good practices' for the protection of personal data by public authorities ([183]).

(123) In light of the accountability requirements and practices described in recitals (114) to (122) of this Decision, the Brazilian framework implements the principle of accountability in a way similar to measures provided for under Sections 3 and 4 of Chapter 4 of Regulation (EU) 2016/679, including by providing for different mechanisms to ensure and demonstrate compliance with the LGPD.

2.5. **Oversight and enforcement**

(124) In order to ensure that an adequate level of data protection is guaranteed in practice, an independent supervisory authority tasked with powers to monitor and enforce compliance with the data protection rules should be in place. This authority should act with complete independence and impartiality in performing its duties and exercising its powers.

([175]) See, for instance, Article 4 paragraph 1, ANPD, Regulation on SMEs, April 2024.
([176]) See, for instance, Article 4 paragraph 2, ANPD, Regulation on SMEs, April 2024.
([177]) ANPD, Regulation on the role of the DPO in relation to the processing of personal data ('DPO Regulation), July 2024. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074.
([178]) Articles 5 and 9, ANPD, DPO Regulation, July 2024.
([179]) Article 18, ANPD, DPO Regulation, July 2024.
([180]) See, ANPD, Report of Instruction N°1/2023 – Telekall Infoservice. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.
([181]) See for instance, ANPD, Report of Instruction N°5/2024 – Ministério da Saúde. Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.
([182]) Article 38, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([183]) Section II, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

2.5.1. *Independent oversight*

(125) In Brazil, the independent supervisory authority in charge of monitoring and enforcing the LGPD is the Agência Nacional de Proteção de Dados – ANPD.

(126) The ANPD was created by Article 55-A of the LGPD and made an independent body through, first a provisional decree, and then a law in 2022 ([184]). The adoption of the law transforming the nature of the ANPD included changes to the LGPD to revoke provisions that subordinated the functioning and financial operations of the ANPD to authorisations to be granted by the Executive under Brazil's Budget law ([185]). The amended provision of the LGPD recognises that the ANPD as a 'special authority, with technical and decision-making autonomy, with its own assets and with headquarters in the Federal District' ([186]).

(127) As an 'authority of special nature', the ANPD has the autonomy to fully perform its legal functions and powers established under the LGPD, including the administrative management of the agency ([187]). This includes the autonomy to manage its spending and hiring ([188]). The ANPD was first created as an 'authority' before becoming an 'agency' in September 2025, bringing its name in line with other 11 regulatory entities enjoying this high degree of independence in Brazil (e.g. the National Agency for Electricity, the National Agency for Telecommunications, etc.) ([189]).

(128) The ANPD's resources are largely derived from the general budget of the Brazilian Federal State. In addition, the budget of the ANPD may include donations, subsidies or other credits as set under Article 55-L of the LGPD. Since its creation in 2021, the ANPD has been growing exponentially. Annual reports from the ANPD indicate that the authority had 141 employees/civil servants at the end of 2023, after only four years of existence ([190]). The 2025 annual budget of the ANPD is R$ 18 million ([191]). In September 2025, the creation of a new civil service career track on 'data protection', with 200 posts, was announced in Brazil, as part of an increase to the ANPD's workforce in the years to come ([192]).

([184]) Article 55-A of Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), in its original wording, has been amended by Law N°14.460 of 25 October 2022, Law transforming the ANPD into an authority of special status. On independence, see Provisional measure N°1.124 of 13 June 2022, transforming the ANPD into an authority of special status. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Mpv/mpv1124.htm and Law N°14.460 of 25 October 2022, Law transforming the ANPD into an authority of special status. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14460.htm. The possibility for the government to change the status of the ANPD to increase its independence was detailed in the (now revoked) Article 55-A, paragraph 1 of Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([185]) See Article 9 of Law N°14.460 of 25 October 2022, Law transforming the ANPD into an authority of special status, revoking and replacing Article 55-A of Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([186]) Article 7, Law N°14.460 of 25 October 2022, Law transforming the ANPD into an authority of special status.

([187]) See ANPD, The ANPD becomes an authority of special nature, June 2022. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial.

([188]) Article 55-L, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([189]) Article 1, Decree N°1.317 of 17 September 2025 modifying the LGPD to transform the Agência Nacional de Proteção de Dados. Available at: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314 and Article 2 (XII), Law N°13.848 of 25 June 2019 on the organisation of regulatory agencies. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13848.htm.

([190]) ANPD, Report on the fourth year of the ANPD, November 2023, p.8. Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view.

([191]) R$ 18 225 566 (EUR 2 857 768). See, Annual Budgetary Law, p. 190. Available at: LEI15121-VOLUME I.pdf.

([192]) Article 9 (I), Decree N°1.317 of 17 September 2025 modifying the LGPD to transform the Agência Nacional de Proteção de Dados. Available at: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

(129) The ANPD is composed of a Board of Directors (which is its highest governing body), a National Council for Personal Data and Privacy Protection (which has advisory powers) and several administrative offices and units ([193]). This structure is established in Article 55-C of the LGPD and further detailed in two decrees adopted in 2020 and 2023, respectively ([194]).

(130) The Board of Directors is comprised of five Directors, including the President of the Authority. Each member of the ANPD's Board of Director is appointed for five years by Brazil's President of the Republic, after approval by the Federal Senate ([195]).

(131) Directors shall be Brazilian and have a high-level of education relevant to the post ([196]). To ensure their independence, all Directors must abstain from any profit-related business, political activities and from holding positions of management or adviser in any companies, among others ([197]). In addition, Brazilian law regulating the exercise of senior positions within the federal public administration establishes that individuals holding functions equivalent to that of the ANPD Directors are prohibited, among other restrictions, from engaging in activities that are incompatible with their duties ([198]). This includes acting as consultants or intermediaries of private interests (even informally) or providing services to entities subject to ANPD's oversight or regulation, even on an occasional basis. Furthermore, at the end of their mandate or tenure at the ANPD and for six months after that, Directors are barred from exercising certain functions that may create risk of conflicts of interest ([199]).

(132) Directors may only be dismissed under specific circumstances defined under Article 55-E of the LGPD, namely 'upon resignation, final and unappealable judicial conviction or dismissal penalty due to disciplinary administrative proceeding'. The Federal Law on Public Office establishes that such a penalty must be justified and can only be proposed in case of demonstrated specific offences (i.e. serious misconduct, corruption, irregular use of public funds) ([200]). These rules and procedure provide the ANPD's Directors with institutional protection in the exercise of their functions. To date no directors of the ANPD was ever dismissed or faced disciplinary proceedings. The ANPD's Board of Director has been in place and remained unchanged through a change of administration in Brazil which took place in 2023.

([193]) Article 55-C, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([194]) Decree N°10.474 of 26 August 2020 on the structure of the ANPD. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm amended by Decree N°11.758 of 30 October 2023 on the amended structure of the ANPD. Available at: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11758.htm#art1.

([195]) Article 55-D, paragraphs 1 and 3, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law and Article 12, Decree N°1.317 of 17 September 2025 modifying the LGPD to transform the Agência Nacional de Proteção de Dados. Available at: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314. Article 12 of this decree extends the length of the ANPD's Directors' mandate from four to five years to align with all other existing independent regulatory agencies in Brazil. All ANPD's Directors that have been named prior to the adoption of this decree will complete a mandate of four years, as initially foreseen by law at the time of their appointment.

([196]) Article 55-D, paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([197]) Article 11, Decree N°10.474 of 26 August 2020 on the structure of the ANPD.

([198]) Article 5, Law N°12.813 of 16 May 2013, Law on conflict of interest for public servant and other role in public authorities. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12813.htm.

([199]) Article 6, Law N°12.813 of 16 May 2013, Law on conflict of interest for public servant and other role in public authorities.

([200]) The complete an exhaustive list of offences can be found in Article 132 of Law N°8112 of 11 December 1990, Federal law on Public Office and Civil Servants. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. See also, Chapter V of this law on the conditions to apply a penalty.

(133) The tasks and powers of the ANPD are detailed in Article 55-J of the LGPD. In particular, they include developing data protection policies and guidelines, promoting the adoption of standards that facilitate the control of data subjects over their personal data, investigating infringements of individual rights, handling complaints, enforcing compliance with the LGPD and issuing sanctions, ensuring education and promotion in the area of data protection, and exchanging and cooperating with third country data protection authorities, among others ([201]).

(134) The ANPD has an advisory body formed by the National Council for Personal Data and Privacy Protection, as established by Article 58-A of the LGPD. This body is composed of representatives of the Executive, Legislative, and Judiciary, as well as of civil society, trade union, and the business sector ([202]). It has a purely advisory role consisting in preparing studies or annual reports on data protection, holding public debates and hearing on personal data protection and privacy, proposing non-binding recommendations to the ANPD and disseminate knowledge on the protection of personal data and privacy ([203]). The cooperation between the ANPD and the National Council is centered on the promotion of data protection and privacy in Brazil. The National Council has no powers in relation to the monitoring and enforcement of the LGPD, as only the ANPD has the authority to oversee the implementation of the law and to enforce it by, for instance, issuing regulations, conducting investigations and applying sanctions. As an independent authority, the ANPD does not have to follow any suggestions that may be presented by the National Council through its reports or non-binding recommendations.

2.5.2. *Enforcement, including sanctions*

(135) To enforce compliance, the legislator has granted the ANPD both investigatory and enforcement powers, ranging from warnings to administrative fines.

(136) As regards investigatory powers, if a violation of the LGPD is suspected or has been reported, or where necessary for the protection of data subject rights that have been/are likely to be infringed, the ANPD may carry out at any time audits and on-site inspections at controllers from the public and private sectors and request any necessary information ([204]). In particular, the binding Regulation on the ANPD's Sanctioning Powers, establishes that the controllers and processors shall allow the ANPD 'access to offices/buildings, equipment, applications, facilities, systems, tools and technological resources, documents, data and information of a technical, operational and other nature relevant to the assessment of personal data processing activities, in its possession or in the possession of third parties' ([205]).

([201]) Article 55-J (I) to (XXIV), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([202]) For more information on the members and activities of the National Council, see ANPD, National Council for Personal Data and Privacy Protection. Available at: https://www.gov.br/anpd/pt-br/cnpd-2.

([203]) Article 58-B, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([204]) Article 55-J (XVI), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Article 4 (I), Decree N°10.474 of 26 August 2020 on the structure of the ANPD, and Article 12, ANPD, ANPD, Regulation on Security Incident Notification, April 2024.

([205]) Article 5, ANPD, Regulation on the Sanctioning Powers of the ANPD, October 2021. Available at: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021.

(137) As part of its corrective powers, the ANPD may impose warnings, fines, or other sanctions such as orders to temporarily stop the processing of data or delete personal data ([206]). These sanctions can be imposed towards public or private entities, with the exception of fines and daily fines which cannot be imposed on public entities ([207]). Several, cumulative sanctions may be applied to bring an entity into compliance. Through a warning, the ANPD would provide a controller with a specific time period to adopt corrective measures in order to bring a processing in compliance with the LGPD ([208]). Failure to do so, would lead to additional sanctions. For instance, the ANPD has issued several warnings to the Ministry of Health for failing to provide a data protection impact assessment and to notify a data breach, among others ([209]). The ANPD can impose several sanctions in conjunction to protect data subjects' rights or to ensure compliance with the LGPD. For instance, the ANPD may impose an administrative fine for a violation of the LGPD alongside with an order to delete data that is linked to this violation ([210]). The ANPD may also, in case of non-monetary sanctions, decide to issue 'daily fines' to 'when necessary to ensure compliance (with the LGPD) within a deadline' ([211]). The daily fine is applied cumulatively, considering the time between the incidence of the fine and the fulfilment of the obligation, and for up to R$ 50 million ([212]).

(138) Pursuant to Article 52 (II) of the LGPD, the ANPD can issue administrative fines, in addition to daily fines, for up to 2 % of an entity's revenue in Brazil, for a maximum of R$ 50 million ([213]). Fines can be cumulative in case of multiple violations. The ANPD issued its first monetary fines, a few months after the adoption of its Regulation on Sanctions towards a telecommunications company which failed to identify a legal basis for processing and to appoint a data protection officer. The company received a warning and two fines for a total of R$ 14 400 ([214]). In the binding Regulation on Sanctions, the ANPD categorised sanctions into three levels of gravity: light, medium, and serious ([215]) depending on established factor such as the type and volume of data processed, the type of processing, or the impact on the data subject's rights. For instance, violations concerning the processing of sensitive personal data are subject to the highest level of sanctions that the ANPD can impose ([216]).

(139) The Regulation on Sanctions provides for a methodology on the calculation on fines, including to take into account aggravating and/or mitigating factors ([217]). For instance, a fine may be increased by 10 per cent in case of repeated specific violations or even 90 per cent for each corrective measure not complied with by a set deadline ([218]). Similarly, a fine may be decreased by 50 per cent if the violation is remedied right after the launch of the administrative proceeding by the ANPD ([219]).

([206]) Articles 55 and 55-J (IV), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) and ANPD, Regulation on Sanctions, February 2023.
([207]) Article 52, paragraph 3. Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([208]) Article 52 (I), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([209]) See, ANPD, Decision N°4/2024, available at https://www.gov.br/anpd/pt-br/centrais-de-conteudo/relatorio_de_instrucao_no_4_2024_fis_cgf_anpd_v-publica.pdf and ANPD, Decision N°5/2024, available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.
([210]) Article 52 (VI), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([211]) Article 16, ANPD, Regulation on Sanctions, February 2023.
([212]) Article 16, paragraph 1, ANPD, Regulation on Sanctions, February 2023. 50 million of Brazilian Reals is approximately EUR 7,8 million.
([213]) 50 million of Brazilian Reals is approximately EUR 7,8 million.
([214]) ANPD, Decision N°1/2023, Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.
([215]) Article 8, ANPD, Regulation on Sanctions, February 2023.
([216]) Article 8, paragraph 3 (I) (d), ANPD, Regulation on Sanctions, February 2023.
([217]) Annex I, Articles 12-13, ANPD, Regulation on Sanctions, February 2023.
([218]) Article 12 (I) to (IV), ANPD, Regulation on Sanctions, February 2023.
([219]) Article 13 (I), ANPD, Regulation on Sanctions, February 2023.

(140) The Brazilian system therefore combines diverse types of sanctions, from corrective measures and administrative fines. Immediately after its sanctioning powers became effective, the ANPD started to make use of its powers ([220]). To date, sanctions and recommendations have been issued against both public authorities, including in the area of security, and private operators ([221]). The sanctions issued by the ANPD to date concerns a wide range of issues, including the lack of appointment of a DPO, security incidents including data breaches, or failure to cooperate with the ANPD. In addition to issuing monetary fines, the ANPD has been particularly active in using the full range of its corrective powers to, for instance, issue orders to controllers to conduct a DPIA or to stop the processing of personal data. For instance, in July 2024, the ANPD issued an order to a large social media platform to suspend the processing of personal data for training generative artificial intelligence (AI) systems in all its products ([222]). Together with this preventive measure, aimed to protect the fundamental rights of data subjects, the ANPD issued daily fine of R$ 50 000 until the processing was brought in compliance with the LGPD ([223]). Lastly, the ANPD has announced the opening of investigations against several large multi-national tech platforms, social media companies and a bank, while continuing investigations against entities of the public sectors ([224]). In its few years of existence, the ANPD has shown a strong record of enforcement, making use of the full range of its enforcement powers.

(141) Lastly, the administrative sanctions established under the LGPD do not replace the application of other administrative or otherwise civil and criminal sanctions, including those set under Brazil's Consumer Protection Code ([225]) and the Civil Framework for the Internet ([226]). In particular, the Brazilian Consumer Protection Code requires companies to provide consumers with information about their businesses and activities ([227]). Article 56 of the Consumer Protection Code further lists the sanctions faced by companies in case of non-compliance which ranges from fines to prohibition to sell or produce a product, or obligation to suspend a service. In addition, Articles 61 to 74 of the Consumer Protection Code list the criminal offences for which companies may face from six months to two years in prison, including in case of false or misleading claims in relation to a service or of promotion of a service that may cause harm to the consumer. For instance, in 2014, Brazil's Department of Consumer Defence and Protection fined a telecommunications company R$ 3,5 million for violations of the Consumer Protection Code and Civil Framework for the Internet in relation to its use of tracking for online behavioural advertising and the sale of browsing data ([228]).

(142) It follows from the above that the Brazilian system ensures an effective enforcement of its data protection rules in practice.

2.5.3. *Redress*

(143) In order to ensure adequate protection and in particular the enforcement of individual rights, the data subject should be provided with effective administrative and judicial redress, including compensation for damages.

([220]) ANPD, Register of Sanctions. Available at: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/decisoes-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

([221]) See, for instance, Technical Note N°175/2023 on the draft Cooperation Agreement between the Ministry of Justice and Public Security and the Brazilian Federation of Football for sharing personal data with a view to improving the 'Safe Stadium Project'. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

([222]) ANPD, Preventative Measure, Vote N°11/2024. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf.

([223]) R$ 50 000 is the equivalent of EUR 7 800.

([224]) The full and updated list of ongoing investigations and cases opened by the ANPD can be found here: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao.

([225]) Law N°8.079 of 11 September 1990, Consumer Protection Law. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

([226]) Law N°12.965 of 23 April 2014, Marco Civil da Internet ('Civil Framework for the Internet'). Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([227]) Article 6, Law N°8.079 of 11 September 1990, Consumer Protection Law.

([228]) R$ 3,50 million was approximately EUR 1,5 million, based on the exchange rate at the time.

(144) The Brazilian system provides individuals with various mechanisms to effectively enforce their rights and obtain redress.

(145) As a first step, individuals who consider that their data protection rights or interests have been violated or want to exercise their data protection rights can turn to the relevant controller. According to Article 9 of the LGPD, the controller shall, among others, provide the contact information to allow the filing of data subjects' request and 'pleadings' ([229]).

(146) In addition, under the LGPD and the Brazilian legal system, several redress avenues are open to individuals who consider that their data protection rights or interests have been violated by the controller or the processor of personal data.

(147) First, any individual who considers that his or her data protection rights or interests have been violated by the controller or processor may file a complaint or report such infringement to the ANPD ([230]). The ANPD has a dedicated page on its website to allow data subjects to file a complaint in case of violation of the LGPD or a petition in case of issues regarding a request made towards a controller concerning their data protection rights ([231]). As explained in recital (138) of this Decision, in response to a complaint, the ANPD may impose a sanction as detailed under Article 52 of the LGPD. The Regulation on the ANPD's Sanctioning Powers established the administrative procedure for its proceedings, including deadlines, procedures governing the right to be heard and publication of the decision ([232]).

(148) The decisions of the ANPD can be challenged by the data subjects by presenting an appeal to the Board of Director of the ANPD within 10 days of receiving the decisions ([233]). As part of their right to an effective remedy, individuals may also appeal decisions of the Board in court, as well as present any recourse against the ANPD for failing to comply with its obligations under the LGPD (including a refusal to handle a complaint or a rejection on substance of a complaint) ([234]).

(149) Second, the ANPD can encourage 'direct conciliation' (mediation) between data subjects and controllers, to prioritise problem resolution and 'damage compensation by the controller' ([235]). These processes do not prevent data subjects from filing complaints or accessing other avenues for redress.

(150) Third, regarding damages, Article 42 of the LGPD establishes an obligation for a controller or processor to remedy 'material, moral, individual, or collective damages to others', resulting from the processing of personal data. Data subjects may bring lawsuit, individually or collectively, to seek redress and compensation for these damages ([236]). The LGPD establishes that a judge has the discretion to 'reverse the burden of proof in favour of the data subject' in particular in cases where 'the production of evidence by the data subject would be overly burdensome' ([237]).

(151) Fourth, when a violation of data subjects' rights falls within the scope of consumer law and consumer relation, the protection afforded in this field apply and can be invoked in court ([238]).

([229]) Article 9, read in conjunction with Article 55-J (V), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([230]) Article 55-J (V), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([231]) See, ANPD, Services for the Data Subjects, Filing a complaint or a petition. Available at: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular.
([232]) Sections II and III, ANPD, Regulation on the Sanctioning Powers of the ANPD, October 2021.
([233]) Article 59, ANPD, Regulation on the Sanctioning Powers of the ANPD, October 2021.
([234]) Article 22, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([235]) Article 17 (VIII), ANPD, Regulation on the Sanctioning Powers of the ANPD, October 2021.
([236]) Article 42, paragraph 3, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([237]) Article 42, paragraph 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([238]) Article 45, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

(152) Fifth, the Brazilian Federal Supreme Court has recognised that individuals have a right to claim injunctive relief for infringements of their rights under the Constitution, including the right to the protection of personal data ([239]). In this context, a court may, for instance, order controllers to suspend or stop any unlawful activity. In addition, data protection rights, including the rights protected by the LGPD, can be enforced via civil actions. Article 22 of the LGPD explicitly allows for the defence of data subject rights to be exercised in court and more broadly for individuals to bring data protection cases to court, either individually or collectively.

(153) The Brazilian system therefore offers various avenues to obtain redress, from easily accessible, low-cost options (e.g. complaints to the ANPD) to judicial avenues, which include the possibility to obtain compensation for damages or to seek collective redress.

3. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN BRAZIL

(154) The Commission also assessed the limitations and safeguards, including the oversight and individual redress mechanisms available in Brazilian law as regards the collection and subsequent use by Brazilian public authorities of personal data transferred to controllers and processors in Brazil in the public interest, in particular for criminal law enforcement and national security purposes (hereafter referred to as 'government access').

(155) In assessing whether the conditions under which government access to data transferred to Brazil under this Decision fulfil the 'essential equivalence' test pursuant to Article 45(1) of Regulation (EU) 2016/679, as interpreted by the Court of Justice of the European Union in light of the Charter of Fundamental Rights, the Commission took into account in particular the following criteria.

(156) First, any limitation to the right to the protection of personal data must be provided for by law and the legal basis which permits the interference with such a right must itself define the scope of the limitation on the exercise of the right concerned ([240]).

(157) Second, in order to satisfy the requirement of proportionality, according to which derogations from and limitations to the protection of personal data must apply only in so far as is strictly necessary in a democratic society to meet specific objectives of general interest equivalent to those recognised by the Union, the legislation of the third country in question which permits the interference must lay down clear and precise rules governing the scope and application of the measures in question and impose minimum safeguards so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse ([241]). The legislation must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted ([242]) as well as subject the fulfilment of such requirements to independent oversight ([243]).

([239]) The Brazilian Federal Supreme Court issued a ruling in 2020 that halted a presidential executive order that would have forced telecom companies to share subscriber data with the census agency, recognising for the first, data protection as a fundamental right, paving the way for the right to be included in Brazil's Constitution. See, Federal Supreme Tribunal, Decision on ADI 6387 of 7 May 2020. Available at: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([240]) Schrems II, paragraphs 174-175, and case-law cited. See also, as regards access by public authorities of Member States, Case C-623/17 'Privacy International', ECLI:EU:C:2020:790, paragraph 65; and Joined Cases C-511/18, C-512/18 and C-520/18 'La Quadrature du Net and Others', ECLI:EU:C:2020:791, paragraph 175.

([241]) Schrems II, paragraphs 176 and 181, as well as the case-law cited. See also, as regards access by public authorities of Member States, Privacy International, paragraph 68; and La Quadrature du Net and Others, paragraph 132.

([242]) Schrems II, paragraph 176. See also, as regards access by public authorities of Member States, Privacy International, paragraph 68; and La Quadrature du Net and Others, paragraph 132.

([243]) Schrems II, paragraph 179.

(158) Third, that legislation and its requirements must be legally binding under domestic law. This concerns first of all the authorities of the third country in question, but these legal requirements must also be enforceable before courts against those authorities ([244]). In particular, data subjects must have the possibility of bringing legal action before an independent and impartial tribunal in order to have access to their personal data, or to obtain the rectification or erasure of such data ([245]).

3.1. **General legal framework**

(159) The limitations and safeguards that apply to the collection and subsequent use of personal data by Brazilian public authorities follow from the overarching constitutional framework, specific laws that regulate their activities in the areas of criminal law enforcement and national security, as well as the rules that specifically apply to the processing of personal data.

(160) First, access to personal data by Brazilian public authorities is governed by the general principle of legality – from which the principles of reasonableness, necessity and proportionality derive – enshrined in the Brazilian Constitution ([246]). In particular, according to Article 5 of the Constitution, fundamental rights and freedoms (including the right to privacy and data protection) may only be restricted by law and when necessary for imperatives of national security, public security, or other specific public interest purpose specified by law. Such restrictions must be reasonable and proportionate ([247]). In particular, the evaluation of public interest purpose is essential for assessing the proportionality of the interference, in light of the principle of legality. Article 5 (LIV) of the Constitution further establishes that 'no one shall be deprived of his/her liberty or property without due process'.

(161) Second, the Brazilian order guarantees *Habeas Data* as a constitutional redress avenue designed to protect the right of access to, rectification, and deletion of personal data held by public authorities or in public datasets or registries ([248]). It serves as a safeguard against the misuse or violation of privacy related to data processing by public entities. Any individuals can initiate a claim or request on the basis of *Habeas Data*, regardless of their nationality ([249]).

(162) Third, the general principles and rights mentioned in recitals (155) to (158) are also reflected in the specific laws that regulate the powers of law enforcement and national security authorities. For example, the Civil Framework for the Internet provides for measures requiring a prior judicial order for access to data and limitation on access to online data ([250]). Similarly, the Telephone Interception Law establishes specific measures and safeguards for the processing of telecommunications data ([251]). In the area of national security, the Law establishing the Brazilian Intelligence System provides for measures for lawful access to data for national security purposes ([252]).

([244]) Schrems II, paragraphs 181-182.

([245]) Schrems I, paragraph 95 and Schrems II, paragraph 194. In that respect, the CJEU has notably stressed that compliance with Article 47 of the Charter of Fundamental Rights, guaranteeing the right to an effective remedy before an independent and impartial tribunal, 'contributes to the required level of protection in the European Union [and] must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of Regulation (EU) 2016/679' (Schrems II, paragraph 186).

([246]) Article 5 (II), 1988 Constitution of the Federative Republic of Brazil.

([247]) Brazil is subject to the jurisdiction to the Inter-American Court of Human Rights which, among others, recognised the principle of proportionality as 'essential in a democratic society' and that limitations to fundamental rights can only occur if intended to meet an imperative public objective. See, e.g. MENDES, Gilmar Ferreira. Fundamental rights and judicial control. São Paulo: Saraiva, 2012, p.78.

([248]) Article 5 (LXXII) and (LXXVII), 1988 Constitution of the Federative Republic of Brazil.

([249]) See also recitals (9) and (11) of this Decision.

([250]) Law N°12.965 of 23 April 2014, Marco Civil da Internet ('Civil Framework for the Internet'). Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([251]) Law N°9.296 of 24 July 1996, Telephonic Interception Law. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

([252]) Law N°9.883 of 7 December 1999. Law establishing the Brazilian Intelligence System.

(163) Fourth, the processing of personal data by public authorities, including for law enforcement and national security purposes, is subject to data protection requirements under the LGPD. As described in recital (31) of this Decision, the exemption concerning the application of the LGPD in the area of public safety, national defence, State security and the investigation and prosecution of criminal offences set under the LGPD is partial. The Federal Supreme Court has interpreted the applicability of the LGPD in light of the constitutional protection of personal data and established that the main principles, rights, and objectives of the LGPD apply to all processing of personal data by public authorities, including when conducted for criminal law enforcement or national security purposes ([253]). On that basis, the ANPD has, for instance, conducted investigations and issued guidance, such as technical note to public authorities for activities related to public safety in which it recalled that processing for these public interest purposes must comply with the general principles and rights provided by the LGPD ([254]).

(164) Finally, individuals can invoke their constitutional rights and freedoms before the Federal Supreme Court if they believe that they have been infringed by public authorities in the exercise of their powers. Individuals can also seek redress, in relation to their data protection rights, before independent oversight bodies (e.g. the ANPD) and courts, as detailed in recitals (143) to (153) of this Decision.

3.2. **Access and use by Brazilian public authorities for criminal law enforcement purposes**

(165) Brazilian law imposes a number of limitations on the access and use of personal data for criminal law enforcement purposes and provides oversight and redress mechanisms which are in line with the requirements referred to in recitals (155) to (158) of this Decision. The conditions under which such access can take place and the safeguards applicable to the use of these powers are assessed in detail in the following sections.

3.2.1. *Legal basis, limitation, and safeguards*

(166) As a general rule, access to personal data by public authorities for criminal law enforcement purposes takes place on the basis of a prior judicial order issued by a competent judicial authority ([255]). As an exception to this rule, it is possible for police and public prosecution authorities, in cases specifically provided for by law, to have access to the data of persons under investigation included in a public register, that is to say, data relating to personal qualification, affiliation and address ([256]). The exhaustive list of accessible registers, provided for by law, cover information of Brazilians or individuals residing in Brazil and would not cover access to data transferred from the EU, thus falling outside the scope of this Decision ([257]). Access to these registers is governed by the constitutional principle of legality – from which the principles of reasonableness, necessity and proportionality derive – and can be subject to *ex post* judicial review, as explained in recitals (159) to (161).

(167) The authorities in Brazil that are entitled to access and collect personal data for criminal purposes, through a prior judicial order are: (1) the Civil Police; (2) the Federal Police; (3) the State Public Prosecutor's Office; (4) the Federal Public Prosecutor's Office; (5) Judges and Courts; and (6) Parliamentary Committees of Inquiry.

([253]) Federal Supreme Court. Decision on ADI 6649, September 2022. Available at: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([254]) Technical Note N°175/2023, paragraph 5.1.

([255]) See, for instance, Article 5 (XII), 1988 Constitution of the Federative Republic of Brazil.

([256]) Articles 15 and 16, Law N°12.850 of 2 August 2013, Law related to criminal organisations and criminal investigations. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

([257]) The accessible registers cover: employment registers, electoral registers, phone registers, financial registers, internet provider registers, credit card registers. Information in these registers include information about individual subscribing these services or using these public services. Articles 15 and 16, Law N°12.850 of 2 August 2013, Law related to criminal organisations and criminal investigations. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

(168) Pursuant to Article 3-B of the Penal Code, a judge 'responsible for monitoring the legality of the criminal investigation and for safeguarding the individual rights', may grant a judicial order for authorising: (1) telephonic interception of communications on computer and connected systems or other forms of communication; (2) the removal of tax, banking, data and telephonic confidentiality; (3) search and seizure at home; and (4) access to secret information; and (5) 'other measures to obtain evidence that restrict the fundamental rights of the person under investigation' ([258]).

3.2.1.1. Interception of communications

(169) The confidentiality of correspondence of electronic and telephone communications is considered as a fundamental right in the Brazilian legal framework ([259]).

(170) Public authorities can access these data only in exceptional cases for the purposes of criminal investigations or prosecution. The interception of communication must always be a subsidiary and exceptional measure, which is only allowed when there are no other means to solve a specific case, as established by the Federal Supreme Court ([260]). The modalities for interception online and telephone communications are covered by the Telephonic Interception Law ([261]).

(171) Article 2 of the Telephonic Interception Law set strict conditions allowing access to communication. Any interception of communication requires a prior judicial authorisation. A valid request for interception shall be presented to a judge by the authorised public authorities, which can either be (1) the relevant police authority, in the context of a criminal investigation; or (2) the representative of the Public Prosecutor's Office, in the context of a criminal investigation and the criminal prosecution ([262]). The interception of telephone communications shall not be authorised in any of the following circumstances, reflecting the requirements of necessity and proportionality: (1) if there is no reasonable evidence of authorship or participation in a criminal offence; (2) if the evidence can be provided by other available means; (3) if the fact investigated constitutes a criminal offence punishable by detention ([263]).

(172) Furthermore, the Telephonic Interception Law requires that the request for interception shall clarify the necessity of the measure ([264]). The prior judicial authorisation shall be substantiated and consider the proportionality of the means used to conduct the interception ([265]). The judge may authorise to access the content of the communications for a maximum of 15 days. This period can be extended by a new judicial decision once the indispensability of the measure is proven ([266]). Any interception of communications, including environmental monitoring, conducted without a judicial authorisation or for purpose not authorised by the law constitute a crime punishable by up to four years in prison ([267]).

([258]) Decree-Law N°3.689 of 3 October 1941, Penal Code. Available at: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([259]) Article 5 (XII), 1988 Constitution of the Federative Republic of Brazil.
([260]) Federal Supreme Court, HC 108147/PR, 2012. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.
([261]) Article 1, Law N°9.296 of 24 July 1996, Telephonic Interception Law.
([262]) Article 2 (I) and (II), Law N°9.296 of 24 July 1996, Telephonic Interception Law.
([263]) Article 2, Law N°9.296 of 24 July 1996, Telephonic Interception Law.
([264]) Article 4, Law N°9.296 of 24 July 1996, Telephonic Interception Law.
([265]) Article 5, Law N°9.296 of 24 July 1996, Telephonic Interception Law.
([266]) Article 5, Law N°9.296 of 24 July 1996, Telephonic Interception Law.
([267]) Article 10, Law N°9.296 of 24 July 1996, Telephonic Interception Law.

(173) As a general rule, data accessed and collected for criminal purposes in accordance with the Telephonic Interception Law will be kept for the duration of processing and then deleted once no longer needed for judicial proceeding, in accordance with the binding guidelines of the Judiciary ([268]). Article 9 of the Telephonic Interception Law further establishes that when the content collected is unrelated to the matter investigated in the case, the data will be rendered 'unusable' ([269]).

(174) Concerning telecommunication metadata, Article 17 of the Law related to criminal organisations and criminal investigations requires phone companies to retain user account information of individuals residing in Brazil and records of phone calls (phone numbers exclusively) for five years ([270]). Access to this registry maintained by ANATEL (Brazil's telecommunication regulatory agency) is restricted to specific public entities and requires a judicial authorisation, as described above.

(175) Concerning information available online, Article 7 of the Civil Framework for the Internet further guarantees 'the inviolability and confidentiality of the flow of communications over the Internet', except by court order, in accordance with the law; and 'the inviolability and confidentiality of stored private communications, except by court order' ([271]).

(176) Pursuant to Article 10 of the Civil Framework for the Internet, access to the content of online communication and to connection data (including metadata) can only take place through a prior judicial order. Pursuant to Article 22 of the Civil Framework for the Internet, the application for a judicial order must include: (lit. i) well-founded evidence of the occurrence of the offence; (lit. ii) reasoned justification of the usefulness of the records requested for investigation or for evidence purposes; and (lit. iii) establish the period to which the records refer. Article 13 further requires internet or application service providers to retain connection logs for one year 'in a controlled and secured environment' ([272]). No similar obligation to retain data exists in relation to the content of online communications. Access to the retained record of connection logs can only be granted to a competent authority on the basis of a judicial authorisation, under the conditions described in this recital ([273]).

(177) Article 11 of the Civil Framework for the Internet recalls that any operation involving the collection, storage, retention or any other processing of logs, personal data or communications by connection providers and internet applications in Brazil, must respect 'Brazilian legislation and the rights to privacy, the protection of personal data and the confidentiality of private communications and records'. It follows from the safeguards reflected in recitals (175) to (177) that mass collection and retention of internet communication data is generally not authorised in Brazil.

3.2.1.2. Removal of tax, banking, data and communications confidentiality protection

(178) There is constitutional protection in Brazil for the confidentiality of correspondence of electronic (including data) and telephone communications ([274]). The LGPD further protects the use of data and communication information ([275]), while the Law on the confidentiality of Financial Institutions protect the confidentiality of tax and banking information ([276]).

([268]) Article 20, Resolution N°324, 20 June 2020. Available at: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/atos-do-poder-judiciario/resolucao-no-324-de-30-de-junho-de-2020.
([269]) Article 9, Law N°9.296 of 24 July 1996, Telephonic Interception Law.
([270]) Article 17, Law N°12.850 of 2 August 2013, Law related to criminal organisations and criminal investigations. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.
([271]) Article 7, Law N°12.965 of 23 April 2014, Marco Civil da Internet ('Civil Framework for the Internet').
([272]) Article 13 main paragraph, Law N°12.965 of 23 April 2014, Marco Civil da Internet ('Civil Framework for the Internet').
([273]) Article 13, Paragraph 5, Law N°12.965 of 23 April 2014, Marco Civil da Internet ('Civil Framework for the Internet').
([274]) Article 5 (XII), 1988 Constitution of the Federative Republic of Brazil.
([275]) See, Article 2, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.
([276]) Complementary Law N°105 of 10 January 2001, Law on the confidentiality of the operations of financial institutions. Available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(179) Public authorities can access this information only in exceptional cases for the purposes of criminal investigations or prosecution. The interception of communication must always be a subsidiary and exceptional measure, which is only allowed when there are no other means to solve a specific case, as established by the Federal Supreme Court ([277]).

(180) The criteria and safeguards for access to data and communications is set under Civil Framework for Internet and the Telephonic Interception Law and are detailed in recitals (169) to (177) of this Decision.

(181) Concerning tax and banking data, Article 1 of the Law on the Confidentiality of Financial Institutions set the conditions for the lifting of the general obligations to guarantee the confidentiality of this information. First, the confidentiality can only be lifted through a judicial authorisation ([278]). Second, the measures can only be authorised for the criminal investigations or prosecution of identified offences or crimes as follows: (1) terrorism; (2) illicit trafficking of narcotic substances or similar drugs; (3) smuggling or trafficking of weapons, ammunition or material intended for their production; (4) extortion through kidnapping; (5) crimes against the national financial system; (6) crimes against the Public Administration; (7) crimes against the tax system and social security; (8) money laundering or concealment of assets; and (9) association with a criminal organisation ([279]). Article 10 of the law further establishes that the confidentiality protection for tax and banking data shall not be lifted for any other purposes and failure to respect this limitation constitute a crime punishable by up to four years in prison ([280]).

3.2.1.3. Searches and seizures

(182) As a general rule, the Federal Constitution provides searches and seizures may only take place under strictly defined exceptional circumstances or as provided by law and on the basis of a judicial order issued by a competent judicial authority and in respect of due process ([281]). Searches and seizures have to comply with the principle of legality and be conducted to the extent necessary.

(183) In the following exceptional circumstances, searches and seizures may take place without a judicial order: (1) in case of *flagrante delicto* (i.e. if a crime is being committed in the presence of law enforcement); (2) in case of a natural disaster (in order to save individuals' lives or properties); or (3) to provide assistance to an individual, unable to provide consent, that requires help ([282]). The case law of Brazil's Federal Supreme Court has clarified that law enforcement authorities may not rely on 'anonymous tips' and 'suspicious behaviour' as ground to conduct searches or seizure without a warrant, as it does not comply with the legality requirement and does not give the authorities a valid justification to breach the inviolability of home ([283]).

(184) In terms of procedural safeguards, in line with Brazil's constitutional principles, no search of electronic device can occur without reasonable suspicion that a criminal offence is stored in the device, and as a general rule, without a judicial order ([284]). Furthermore, an individual cannot be forced to hand over data if such handing over could breach the individual's constitutional rights, such as the right to not incriminate oneself ([285]). In submitting a

([277]) Federal Supreme Court, HC 108147/PR, 2012. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.
([278]) Article 3-B, Decree-Law N°3.689 of 3 October 1941, Penal Code. Available at: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([279]) Article1, paragraph 4 (I) to (IX), Complementary Law N°105 of 10 January 2001, Law on the confidentiality of the operations of financial institutions. Available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.
([280]) Article 10, Complementary Law N°105 of 10 January 2001, Law on the confidentiality of the operations of financial institutions. Available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.
([281]) Article 5 (XI), 1988 Constitution of the Federative Republic of Brazil.
([282]) Article 5 (XI), 1988 Constitution of the Federative Republic of Brazil.
([283]) Federal Supreme Court, 2020, Case J.S. Extraordinary Appeal No. 603616.
([284]) Article 5 (XI), 1988 Constitution of the Federative Republic of Brazil.
([285]) Article 5 (LXIII), 1988 Constitution of the Federative Republic of Brazil. See also, Decree-Law No. 2.848 of 7 December 1940, Criminal Procedure Code. Available at: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

request for a search order to court, the criminal law enforcement authority shall provide the relevant facts and evidence supporting the need to access the computer system and data, using lawfully acquired access credentials ([286]). In case the court grant the search order, the authorities will use the access credentials to access the computer system and data therein, in accordance with the terms and conditions specified in the order. Once the search or access is completed, the competent authorities must submit a report to the court, describing the results of the search or access, and providing a list of the data or information obtained.

3.2.1.4. Access to confidential information

(185) Article 4 of the Law on Access to Information ('LAI') defines 'confidential information' as information that 'is temporarily subject to restriction of public access due to its essential nature for the security of society and the State' ([287]). Personal data may be part of the scope of confidential information as defined in the previous sentence.

(186) Article 6 of the LAI requires public entities to protect confidential information and to restrict its access. As for access to communication, data, banking, and tax information, access to confidential information for criminal investigations and prosecutions can only take place on the basis of a judicial authorisation, in exceptional cases, and is only allowed when there are no other means to solve a specific case, as established by the Federal Supreme Court and by law ([288]).

3.2.1.5. Other measures to obtain evidence that restrict the fundamental rights of the person under investigation

(187) 'Other measures to obtain evidence that restrict the fundamental rights of the person under investigation' refer, for instance, to the possibility to order preventive detention or to put an individual under physical surveillance. These measures are in principle not relevant in the context of transfer of data based on an adequacy decision.

(188) For sake of completeness, such measures, proposed by a public authority, can only be conducted on the basis of a judicial authorisation. The proposed measures must comply with the principle of legality established in the Constitution, be ordered in exceptional cases, and when no other alternative may be used, as established by the Federal Supreme Court.

3.2.2. *Further use of the information*

(189) As regards the subsequent use of personal data for another purpose by a public authority, Article 9 of the Telephonic Interception Law establishes that when the content collected is unrelated to the matter investigated in a specific investigation, the data will be rendered 'unusable'. Article 13 of the Civil Framework for the Internet also limit the retention of connection data in registry to a maximum of one year. Article 10 of the Law on confidentiality of Financial Institutions also limit the purpose for which the confidentiality of tax and banking data may be lifted ([289]). These measures in practice limit the possibility of any further use of information.

([286]) Article 240, Decree-Law No. 2.848 of 7 December 1940, Criminal Procedure Code.
([287]) Article 4 (III), Law N°12.527 of 18 November 2011, Law on Access to Information.
([288]) Federal Supreme Court, HC 108147/PR, 2012. Available at: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401 and Article 3-B, Decree-Law N°3.689 of 3 October 1941, Penal Code. Available at: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([289]) Article 10, Complementary Law N°105 of 10 January 2001, Law on the confidentiality of the operations of financial institutions. Available at: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(190) Moreover, and importantly, the Federal Supreme Court ruled that the LGPD applies to the sharing of personal data between public bodies, including when shared between law enforcement and intelligence agencies ([290]). In particular, the Court recalled that 'the sharing of personal data between public administration bodies and entities presupposes: (1) the definition of a legitimate, specific and explicit purpose for data processing; (2) the compatibility of the processing with the informed purposes; (3) limiting the sharing to the minimum necessary to meet the informed purpose; as well as full compliance with the requirements, safeguards and procedures laid down in the LGPD, in so far as it is compatible with the public sector'. The Court added that 'the processing of personal data carried out by public bodies contrary to the legal and constitutional parameters will trigger the civil liability of the State for damage sustained by individuals' in accordance with Article 42 of the LGPD.

(191) Concerning the sharing of personal data between criminal law enforcement authorities in Brazil and similar authorities in third countries, these activities are governed by instruments of international law, in line with the LGPD. In this regard, Article 33 (III) of the LGPD establishes that international data transfers may take place when 'necessary for international legal cooperation between public bodies of intelligence, investigation, and prosecution, in accordance with international legal instruments.' In Brazil, the Ministry of Justice and Public Security serves as the central authority for international legal cooperation in criminal matters. The Ministry is responsible for receiving, analysing, transmitting, and monitoring the execution of requests for international cooperation with foreign authorities, in compliance with applicable rules of international law and the LGPD. The processing of personal data necessary for international legal cooperation is subject to the principles of purpose limitation (Article 6 (I) of the LGPD), lawfulness and fairness of processing (Articles 6 and 7 of the LGPD), data minimisation and accuracy (Article 6 (III) and (V) of the LGPD), transparency (Article 6 (VI) of the LGPD), data security (Article 6 (VII) of the LGPD) and storage limitation (Articles 6 (I), (III), (IV) and 16 of the LGPD). Possible disclosure of personal data to third parties (including third countries) can only take place in accordance with these principles, after having assessed compliance with the constitutional principles of necessity and proportionality and ensuring the continuity of protection and compliance with data subjects rights (Article 2 of the Data Transfer Regulation).

(192) The powers of criminal law enforcement authorities in Brazil to collect and access data are therefore circumscribed by clear and precise rules provided for by law and are subject to a number of safeguards. These safeguards comprise in particular guaranteed oversight of the execution of such measures, including through prior judicial approval and safeguards limiting the duration of access and the retention of the information in line with the principles of necessity and proportionality.

3.2.3. *Oversight*

(193) In Brazil, the activities of criminal law enforcement authorities are supervised by different bodies.

(194) First, as confirmed by the Federal Supreme Court, the ANPD is empowered to supervise processing of personal data carried out by criminal law enforcement authorities under certain requirements of the LGPD ([291]). In this context, the ANPD can exercise the investigative and corrective powers it has under the LGPD. For example, the ANPD has investigated the activities of the Federal Police, the Ministry of Justice and Public Security, and other public bodies carrying out Federal, State, or local security activities or having law enforcement responsibilities ([292]). Investigations can be conducted on the basis of ANPD's own volition or following requests and complaints, which can for example be lodged by individuals, civil society organisations, and public authorities. The ANPD for instance conducted several investigations on the use of video-camera following requests from civil society ([293]).

([290]) Federal Supreme Court. Decision on ADI 6649, September 2022. Available at: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([291]) See recital (163) of this Decision and Federal Supreme Court, Decision on ADI 6649 of 15 September 2022. Available at: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([292]) See ANPD, Inspections, including case 00261.000836/2021-76 and 00261.001028/2021-26. Available at:https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340.

([293]) See, ANPD, Inspections, Case 00261.002211/2022-20 related to the use of security camera by authorities in the city of Fortaleza. Request issued to ANPD available at: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos/arquivos-processos-de-fiscalizacao-concluidos/processosesec_pblico00261-002211_2022-20.pdf.

(195) Second, the activities of criminal law enforcement authorities are supervised by the judiciary. Courts have the power to authorise the collection of and access to personal data, in the circumstances mentioned above in recitals (165) to (187). They further have the power to impose civil and criminal penalties in the event of abuse or non-compliance with the legislation in force, which include detention or order to stop certain activities.

(196) Third, the Public Prosecutor's Office, an independent and permanent institution in Brazil that is responsible for defending the legal order and the democratic system has the power to exercise external control over police activities ([294]). As set in the Resolution regarding the Public Prosecutor's Office, the purpose of the external control of police activities is to maintain the 'regularity and adequacy of the procedures employed in carrying out police activities', with particular regard to the 'respect for the fundamental rights guaranteed by the Federal Constitution and laws' ([295]). In this capacity, the Public Prosecutor's Office can, among others, carry out on-site visit, either scheduled or at any time, examine investigations, supervise the seizure of goods, and monitor compliance with warrants ([296]). Any violation of the law shall be reported to court. As part of its roles, the Public Prosecutor's Office has been involved in investigating and prosecuting cases of police violence, abuse of power, and human rights violations. In addition, the Public Prosecutor's Office has a role in overseeing data protection by initiating or joining legal actions on the basis of constitutional protections and promoting data protection rights alongside the ANPD. The Public Prosecutor's Office, for instance, presented its argument to the Federal Supreme Court that supported landmark decision recognising data protection as a fundamental right in Brazil ([297]). A registry of the Public Prosecutor's Office actions concerning the LGPD is also available on their webpage ([298]).

3.2.4. *Redress*

(197) The Brazilian system offers different judicial and administrative avenues to obtain redress, including compensation for damages. These mechanisms provide data subjects with effective administrative and judicial remedies, enabling them in particular to enforce their rights, including the right to have access to their personal data, or to obtain the rectification or erasure of such data.

(198) First, individuals may seek redress in court, including for damages. The Federal Constitution and the Civil Procedure Code provide the legal bases for claiming compensation for non-material damage or material damage caused by the public authority which has unlawfully collected or used data for criminal purposes ([299]). In particular, the Constitution expressly mentions that the right to privacy involves a 'right to compensation' for the material or non-material damage resulting from its infringement ([300]). Court decisions may be appealed to the Federal Supreme Court, and further to the Inter-American Court of Human Rights. In 2009, Brazil was ordered by the Inter-American Court of Human Rights to compensate workers of farming cooperatives due to improper telephone interception operations carried out in the State of Paraná in 1999 in violation of the Telephone Interception Law and of the American Convention on Human Rights ([301]).

([294]) Article 127, 1988 Constitution of the Federative Republic of Brazil.
([295]) Article 20, Resolution 20 of 28 May 2007, External control of police activities. Available at: https://www.cnmp.mp.br/portal/images/Comissoes/CSP/Resolu%C3%A7%C3%B5es_/Resolu%C3%A7%C3%A3o_20.pdf.
([296]) Article 4, Resolution 20 of 28 May 2007, External control of police activities.
([297]) See recital (199) of this Decision and Federal Supreme Court, Decision on ADI 6.387, May 2020. Available at: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.
([298]) Public Prosecutor's Office, 'LGPD at the Public Prosecutor's Office'. Available at: https://www.mpf.mp.br/servicos/lgpd/lgpd-no-mpf.
([299]) See, for instance, Article 43 of Law N°10.408 of 10 January 2002. Civil Procedure Code. Available at: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm.
([300]) Article 5 (X), 1988 Constitution of the Federative Republic of Brazil.
([301]) Inter-American Court of Human Rights, Case Escher et al. v. Brazil Preliminary Objections, Merits, Reparations and Costs. Judgement of 6 July 2009. Available at http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

(199) Second, individuals, no matter their nationality, may rely on protection established by the concept of *Habeas Data* to further obtain access and rectification of their data held by public authorities ([302]). On this basis, individuals can also file cases in front of courts, including 'Direct Action of Unconstitutionality' (Ação Direta de Inconstitucionalidade – 'ADI') at the Federal Supreme Court. The 2020 landmark ruling from the STF that pave the way for Brazil to recognised data protection as a fundamental right was initiated by ADIs filed based on the principle of *Habeas Data* ([303]). The Public Prosecutor's Office was also involved in the case, supporting the position of individuals and civil society that filed the case. The case challenged an Executive Order which aimed to share personal data of over 200 million telecom subscribers with the Brazilian Institute of Geography and Statistics during the COVID-19 pandemic ([304]). The STF found the Executive Order to be in violations of the fundamental rights to privacy and confidentiality of communication protected by the Constitution ([305]). The Executive Order was suspended and the STF ruled that data protection should be considered and protected as a fundamental right, similarly to the right to privacy ([306]). At the time of the decision the LGPD was not yet in force. Therefore, the panel of judges used comparative law, notably case law from the German Federal Constitutional Court and Article 8 of the Charter of Fundamental Rights of the European Union to support their understanding about the unconstitutionality of the Executive Order as well as an interpretation of fundamental rights to dignity and privacy guaranteed in the Constitution and the recognition of the *Habeas Data* as a tool to protect the right to informational self-determination ([307]).

(200) Third, individuals can seek redress towards the ANPD for violations of the LGPD pursuant to its Article 55-J (V) and under the conditions detailed in recitals (146) and (149) of this Decision. Individuals may also exercise their data protection rights established under the LGPD towards public authorities ([308]).

(201) The redress mechanisms described in recitals (197) to (200) of this Decision provide data subjects with effective administrative and judicial remedies, enabling them in particular to enforce their rights, including their data protection right in relation to such data.

3.3. **Access and use by Brazilian public authorities for national security purposes**

(202) The laws of Brazil contain a number of limitations and safeguards with respect to the access and use of personal data for national security purposes, and provides oversight and redress mechanisms which are in line with the requirements referred to in recitals (156) to (158) of this Decision. The conditions under which such access can take place and the safeguards applicable to the use of these powers are assessed in detail in the following sections.

([302]) See recitals (9) and (161) of this Decision.

([303]) Federal Supreme Court, Decision on ADI 6.387, May 2020. Available at: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([304]) Suspended Executive Order N°954 of 17 April 2020. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm.

([305]) Federal Supreme Court, Decision on ADI 6.387, May 2020, p. 12.

([306]) Federal Supreme Court, Decision on ADI 6.387, May 2020, p. 8.

([307]) See, Federal Supreme Court, Decision on ADI 6.387, May 2020, p. 4 and International Bar Association, The impact of Covid-19 for data protection in Brazil: the perspective of Brazil's supreme court. Available at: https://www.ibanet.org/article/82b25a81-7422-4f07-aaa8-9c2db19e22af#:~:text=On%206%20and%207%20May%202020%2C%20the,as%20an%20independent%20fundamental%20right%20in%20Brazil.&text=The%20processing%20of%20data%20is%20allowed%20only,legal%20principles%2C%20such%20as%20transparency%20and%20security.

([308]) Article 23, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

3.3.1. *Legal bases, limitations, and safeguards*

(203) In Brazil, personal data may be accessed for national security purposes as part of intelligence activities on the basis of the Law establishing the Brazilian Intelligence System (SISBIN) ([309]). As a general rule, Article 1 of this law establishes that the Brazilian Intelligence System 'must comply with and preserve the individual rights and guarantees and other provisions of the Federal Constitution, treaties, conventions, agreements, and international commitments to which the Federative Republic of Brazil is a party or signatory' ([310]). This includes guaranteeing the principles of necessity and proportionality, as well as the right to data protection ([311]). The activities to be conducted by the Brazilian Intelligence System are further described in binding decrees ([312]).

(204) Pursuant to Article 4 of the Law establishing the Brazilian Intelligence System, the entities forming part of SISBIN may obtain and analyse specific data for national security purposes ('Segurança Pública'). The concept of national security is governed by a 2021 law that modified the Penal Code ([313]) and which revoked Brazil's Law on National Security ([314]). The 2021 law established an exhaustive list of 'crimes' against national security which frames such notion. These crimes are (1) 'crimes against 'national sovereignty' (which covers act of war, invasion of the county, attempt to seize part of the national territory to form a new country, sharing classified information with foreign governments or foreign criminal organisation which could risk the constitutional order of national sovereignty, and facilitating or forging access to information systems to unauthorised persons) ([315]); (2) crimes against the 'democratic institutions' (which covers violent attempt to end the rule of law by preventing or limiting constitutional powers and coup d'état) ([316]); (3) crimes against the 'functioning of the democratic institutions during the electoral process' (which covers interrupting the electoral process and limiting or imputing through violence individuals' ability to exercise their political rights) ([317]); and (4) crimes against the functioning of the essential services (which covers sabotage of means of public communications, defence facilities, with the aim to end the rule of law) ([318]). Article 359-T of the law clarifies that the exercise of freedom of expression, constitutional rights and powers, the conduct of journalistic activity, including 'through marches, meetings, strikes, gatherings, or any other form of political demonstration with social purposes' cannot be considered a crime ([319]). Brazil's National Intelligence Policy (PIN) set a series of key objectives for intelligence that authorities must consider, such as the prevention of 'sabotage' or 'espionage' ([320]). As a 'high level orientation document', the PIN does not however expand the list of crimes related to the concept of national security nor does it alter its definition ([321]).

([309]) Law N°9.883 of 7 December 1999. Law establishing the Brazilian Intelligence System. Available at: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

([310]) Article 1, paragraph 1, Law N°9.883 of 7 December 1999. Law establishing the Brazilian Intelligence System.

([311]) See recital (160) of this Decision.

([312]) Decree N° 8.793/2016 of 29 June 2016 on the National Intelligence Policy. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm and Decree N° 4.376/2002 of 13 September 2002 on the organisation and functioning of the Brazilian Intelligence System. Available at: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/decreto-no-4-376-de-13-de-setembro-de-2002-seopi_eng_rev-d.pdf.

([313]) Law N°14.197 of 1 September 2021, Law modifying the Penal Code and revoking the 1983 Law on National Security. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm.

([314]) Revoked Law N°7.170 of 14 December 1983, Law on National Security. Available at: https://www.planalto.gov.br/ccivil_03/LEIS/L7170.htm.

([315]) Chapter I, Law N°14.197 of 1 September 2021, Law modifying the Penal Code and revoking the 1983 Law on National Security.

([316]) Chapter II, Law N°14.197 of 1 September 2021, Law modifying the Penal Code and revoking the 1983 Law on National Security.

([317]) Chapter III, Law N°14.197 of 1 September 2021, Law modifying the Penal Code and revoking the 1983 Law on National Security.

([318]) Chapter IV, Law N°14.197 of 1 September 2021, Law modifying the Penal Code and revoking the 1983 Law on National Security.

([319]) Article 359-T, Law N°14.197 of 1 September 2021, Law modifying the Penal Code and revoking the 1983 Law on National Security.

([320]) Article 3, Decree N° 8.793/2016 of 29 June 2016 on the National Intelligence Policy. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

([321]) Introduction, first paragraph, Decree N° 8.793/2016 of 29 June 2016 on the National Intelligence Policy. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

(205) Data that may be accessed and analysed to prevent the above-listed crimes against national security cover information that the public authorities' part of SISBIN have accessed to in the context of their operations and in accordance with the conditions described in recitals (165) to (187) of this Decision (i.e. on the basis of a judicial authorisation delivered for a clearly defined purpose). The data shared with SISBIN is processed through a secure encrypted electronic system with access logs to ensure traceability and auditability of information ([322]). As clarified by the Federal Supreme Court, the sharing of data with SISBIN is subject to the principles of the LGPD, including purpose limitation (Article 6 (I) of the LGPD), data minimisation and accuracy (Article 6 (III) and (V) of the LGPD), transparency (Article 6 (VI) of the LGPD), data security (Article 6 (VII) of the LGPD) and storage limitation (Articles 6 (I), (III), (IV) and 16 of the LGPD) ([323]).

(206) Article 2 of the Law establishing the Brazilian Intelligence System indicates that only public authorities are part of this system. SISBIN is made up of the Brazilian Intelligence Agency (ABIN) and of representatives of Intelligence centres, ministries, secretariats, and agencies of the Federal Public Administration. The list of authorities which are members of SISBIN is provided for in a decree on the organisation and functioning of the system ([324]).

(207) ABIN is the central body of the Intelligence System and is responsible for planning, executing, coordinating, supervising, and overseeing the intelligence activities. These activities must be carried out using confidential means and techniques based on information. To carry out its duties, ABIN receives specific information and data from the different public authorities that are part of SISBIN related to national security. The authorities that are part of SISBIN are required to provide this information ([325]), as the law does not authorise ABIN to collect information on its own. The lawfulness of the data sharing obligation from members of SISBIN was challenged in front of the Federal Supreme Court ([326]). In its ruling issued in 2021, the STF clarified that the data that public authorities share with ABIN must observe the strict public interest purposes (e.g. defence of public institutions and national interest) and it recalled that the specific and legitimate purpose of each data sharing activity is defined through formal procedure subject to and defined in a judicial authorisation ([327]). These limitations also apply to any further sharing of data between public authorities ([328]).

(208) Finally, the processing of data carried out through SISBIN must protect the information from the access of non-authorised persons or bodies. Article 5 of the decree on the functioning of SISBIN explicitly requires that the coordination and sharing of data among authorities' members of the system shall observe 'the legislation regarding professional secrecy and security, the protection of personal data and the security of information and knowledge',

([322]) See SISBIN booklet, 2024, p 18. Available at: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

([323]) Federal Supreme Court. Decision on ADI 6649, September 2022. Available at: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([324]) Article 7, Decree N°11.693 of 6 September 2023 on the organisation and functioning of SISBIN. Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm. Examples of authorities' member of SISBIN include: the Intelligence Centre of the Ministry of Defense, the Directorate for Penitentiary Intelligence of the National Secretariat of the Ministry of Justice and Public Security, the Secretariat-General of External Relations of the Ministry of Foreign Affairs and the Directorate for Intelligence of the Federal Police.

([325]) Article 4, Law N°9.883 of 7 December 1999. Law establishing the Brazilian Intelligence System. Available at: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

([326]) Federal Supreme Court, Decision on ADI 6529 of 15 October 2021. Available at: https://www.jusbrasil.com.br/jurisprudencia/stf/1303041724/inteiro-teor-1303041733.

([327]) Federal Supreme Court, Decision on ADI 6529 of 15 October 2021, p. 22.

([328]) Federal Supreme Court, Decision on ADI 6529 of 15 October 2021, p. 3.

which includes the LGPD as the main legislation in Brazil for the protection of personal data ([329]). Article 6 of the decree further specifies that the information exchanged by authorities in SISBIN shall abide by 'the principle of legal certainty, necessity, the public interest' and have a legitimate aim ([330]). SISBIN also recognises the importance of complying with the LGPD in its public materials and internal procedures ([331]).

(209) The powers of authorities processing data for national security purposes in Brazil are therefore circumscribed by clear and precise rules provided for by law and are subject to a number of safeguards. These safeguards comprise in particular guaranteed oversight of the execution of such measures, including through prior judicial approval and safeguards limiting the access of the information in line with the principles of necessity and proportionality.

3.3.2. *Further use of information*

(210) The processing of personal data collected by Brazilian authorities for national security purposes is subject to the principles of purpose limitation (Article 6 (I) of the LGPD), lawfulness and fairness of processing (Articles 6 and 7 of the LGPD), data minimisation and accuracy (Article 6 (III) and (V) of the LGPD), transparency (Article 6 (VI) of the LGPD), data security (Article 6 (VII) of the LGPD) and storage limitation (Articles 6 (I), (III), (IV) and 16 of the LGPD).

(211) Possible disclosure of personal data to third parties (including third countries and through international agreements) can only take place in accordance with the LGPD principles, after having assessed compliance with the constitutional principles of necessity and proportionality and ensuring the continuity of protection and compliance with data subjects rights (Article 2 of the Data Transfer Regulation).

3.3.3. *Oversight*

(212) The activities of Brazilian national security authorities are supervised by different bodies. The decree on Brazil's National Intelligence Strategy notes the importance of having several layers of oversight mechanism to protect the 'democratic rule of law' ([332]). The Federal Supreme Court recalled the importance of this oversight in a case regarding the processing of data under SISBIN, stating that 'the effectiveness of intelligence activities is often linked to the secrecy of the process and the information collected. In the democratic rule of law, this function is subject to the external control of the legislative power and the judiciary in order to assess whether the secrecy imposed is appropriate to the strict public aims to which it is addressed' ([333]).

(213) First, there is control by the Executive Branch, ensuring that the objectives to be achieved by the Intelligence System as well as the policies to be implemented and the plans formulated respond adequately to societal demands. The Executive is also responsible for ensuring that the spending of intelligence services is carried out rationally and exclusively for legitimate, necessary, and useful actions for the State. In the Brazilian framework, this control is exercised by the Chamber of External Relations and National Defence of the Council of Government, which is responsible for overseeing the implementation of the Intelligence National Police, and by the Institutional Security Office, which is responsible for coordinating the activity of federal intelligence ([334]).

([329]) Article 5, Decree N°11.693 of 6 September 2023 on the organisation and functioning of SISBIN.
([330]) Article 6, Decree N°11.693 of 6 September 2023 on the organisation and functioning of SISBIN.
([331]) See, for instance, SISBIN booklet, p. 9: 'One of the objectives of this repositioning is to increase the levels of traceability and transparency of SISBIN's internal processes through the adoption of tools and digital platforms specifically designed for these purposes. These tools must be aligned with the legal framework established by the Access to Information Act and the General Data Protection Law (LGPD), both enacted in 2012'. Available at: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.
([332]) Section 2.4, 4th paragraph, Decree of 15 December 2017 on a National Intelligence Strategy.
([333]) Federal Supreme Court, Decision of 15 October 2021, p. 2.
([334]) Section 2.4, Decree of 15 December 2017 on a National Intelligence Strategy. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm.

(214) Second, the Legislative Branch exercises control as regards intelligence activities. The purpose of that control is to verify both the legitimacy and the effectiveness of the intelligence activity. The heads of the majority and minority parties in the Chamber of Deputies and the Federal Senate, as well as the Chairs of the Committees for External Relations and National Defence of the Chamber of Deputies and the Federal Senate, are part of the external oversight body of intelligence activities called the Joint Committee for the Control of Intelligence Activities ('Comissão mista de Controle da Atividade de Inteligência – CCAI') ([335]). The control of the Legislative Branch over intelligence activities was set through the Law establishing the Brazilian Intelligence System in 1999 and the oversight role and powers of CCAI was significantly strengthen with the adoption of a 2013 binding resolution from Congress ([336]). This resolution addressed previously identified shortcomings to further institutionalised CCAI by providing it with a permanent structure and secretariat, bringing clarity over its powers and increasing transparency over its activities. The role, activities and powers of CCAI are detailed in this resolution and by law. The CCAI monitors and controls the activities of intelligence carried out by bodies of the federal public administration, in particular the bodies forming part of SISBIN, with a view to ensuring that the activities are carried out in accordance with the Constitution and in order to protect the rights and guarantees of individuals, society and the State ([337]). The CCAI can conduct *post hoc* review but also audits and controls of operations in progress ([338]). Members of CCAI have maximum clearance to access documents. The CCAI produces annual reports of its activities, without including information which may endanger national security ([339]). As detailed in recital (222) of this Decision, the CCAI can also receive and investigate complaints from individuals.

(215) Third, the ANPD oversees compliance by national security authorities in relation to the processing of personal data, within the parameters defined by the LGPD. The LGPD partially applies to the processing of personal data carried out for the purposes of public security, national defence, State security or activities investigating and prosecuting criminal offences ([340]). In this context, the ANPD can exercise the investigative and corrective powers it has under the LGPD. The ANPD can for instance carry out audits at any time of all public authorities, including the intelligence agency ([341]).

(216) Finally, the Judiciary will adjudicate lawsuits from citizens against public authorities and in this context, may oversee the activities conducted for national security purposes to ensure compliance with all constitutional rights and the relevant legislative framework, including the LGPD. Court decisions may be appealed to the Federal Supreme Court, and further to the Inter-American Court of Human Rights.

3.3.4. *Redress*

(217) The Brazilian system offers different judicial and administrative avenues to obtain redress, including compensation for damages. These mechanisms provide data subjects with effective administrative and judicial remedies, enabling them in particular to enforce their rights, including the right to have access to their personal data, or to obtain the rectification or erasure of such data.

([335]) Article 6 paragraph 1, Law N°9.883 of 7 December 1999. Law establishing the Brazilian Intelligence System.

([336]) Resolution N°2 of 2021-CN on the Comissão mista de Controle da Atividade de Inteligência (CCAI). Available at: https://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-publicacaooriginal-141944-pl.html.

([337]) Section 2.4, Decree of 15 December 2017 on a National Intelligence Strategy.

([338]) See, in particular, Article 3, Resolution N°2 of 2021-CN on the Comissão mista de Controle da Atividade de Inteligência (CCAI).

([339]) Article 13, Resolution N°2 of 2021-CN on the Comissão mista de Controle da Atividade de Inteligência (CCAI).
Information about meetings and documents prepared by CCAI are available online and regularly updated, available at: https://legis.senado.leg.br/atividade/comissoes/comissao/449/ and https://www.congressonacional.leg.br/legislacao-e-publicacoes/glossario-legislativo/-/legislativo/termo/comissao_mista_de_controle_das_atividades_de_inteligencia_ccai_cn.

([340]) Article 4, Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

([341]) Article 55-J (XI), Law N°13.709 of 14 August 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) – General Data Protection Law.

(218) As detailed in recital (9) of this Decision, access to redress is guaranteed for Brazilian and third country nationals, independently of whether or not they are on the national territory.

(219) First, individuals have an 'absolute' right to bring a lawsuit regarding the protection of their rights. Pursuant to the general rules set in the Civil Procedure Code, to bring an action in court, an individual does not have to demonstrate harm (i.e. that an individual does not have to demonstrate that he/she may be subject to surveillance or that her/his data was processed for national security purposes). The individual may exercise its rights under *Habeas Data* in relation to data processed by intelligence authorities ([342]).

(220) When seeking redress in court, individuals may seek damages. In the same manner as in relation to processing for criminal law enforcement purposes, the Federal Constitution and the Civil Procedure Code provide the legal bases for claiming compensation for non-material damage or material damage caused by the public authority which has unlawfully collected or used data, including through collective actions ([343]).

(221) Second, the Federal Supreme Court has confirmed the partial application of the LGPD to national security purposes, and by extension, the powers of the ANPD to handle complaints related to the processing of personal data by public authorities for purposes of national security ([344]). In the same ruling, the Court noted that 'the processing of personal data carried out by public bodies contrary to the legal and constitutional parameters will require the civil liability of the State for damage sustained by individuals' in accordance with Article 42 of the LGPD ([345]).

(222) Third, the CCAI can receive and investigate complaints about violations of fundamental rights and guarantees committed by public bodies and entities carrying out intelligence and counter-intelligence activities by any citizen, political party, or association ([346]). On this basis, the CCAI may conduct controls or investigations. The CCAI therefore provides for an additional administrative avenue for redress in case of violations of rights related to the processing of data for national security purposes. The complaints received by CCAI can then be further transmitted to courts.

(223) The different judicial remedies available under the Brazilian regime allow individuals to obtain redress. In particular, individuals may challenge the legality of actions of public and intelligence authorities. In addition, they may obtain compensation for damages.

4. **CONCLUSION**

(224) The Commission considers that the Federative Republic of Brazil – through the LGPD – ensures a level of protection for personal data transferred from the European Union that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.

(225) Moreover, the Commission considers that, taken as a whole, the oversight mechanisms and redress avenues in Brazilian law enable possible infringements of the data protection rules by controllers and processors in Brazil to be identified and addressed in practice and offer legal remedies to the data subject to obtain access to his/her personal data and, eventually, the rectification or erasure of such data.

([342]) See recital (9) of this Decision.

([343]) See, for instance, Article 43 of Law N°10.408 of 10 January 2002. Civil Procedure Code. Available at: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm and Article 1, Law N°7.397 of 24 July 1985, Law on civil responsibility. Available at: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm.

([344]) See recitals (31) and (162) of this Decision and Federal Supreme Court, Decision on ADI 6649 of 15 September 2022. Available at: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([345]) Federal Supreme Court, Decision on ADI 6649 of 15 September 2022, point 8. Available at: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([346]) Article 3 (XI), Resolution N°2 of 2021-CN on the Comissão mista de Controle da Atividade de Inteligência (CCAI).

(226) Finally, on the basis of the available information about the Brazilian legal order, the Commission considers that any interference in the public interest, in particular criminal law enforcement and national security purposes, by Brazilian public authorities with the fundamental rights of individuals whose personal data are transferred from the European Union to Brazil will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists.

(227) Therefore, in the light of the findings of this Decision, it should be decided that Brazil ensures an adequate level of protection within the meaning of Article 45 of Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union, for personal data transferred from the European Union to data controllers and processors in Brazil subject to the LGPD.

5. EFFECT OF THIS DECISION AND ACTION OF DATA PROTECTION AUTHORITIES

(228) Member States and their organs are required to take the measures necessary to comply with acts of the Union institutions, as the latter are presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality.

(229) Consequently, a Commission adequacy decision adopted pursuant to Article 45(3) of Regulation (EU) 2016/679 is binding on all organs of the Member States to which it is addressed, including their independent supervisory authorities. In particular, transfers from a controller or processor in the European Union to controllers or processors in Brazil may take place without the need to obtain any further authorisation.

(230) It should be recalled that, pursuant to Article 58(5) of Regulation (EU) 2016/679 and as explained by the Court of Justice in the Schrems I judgment, where a national data protection authority questions, including upon a complaint, the compatibility of a Commission adequacy decision with the fundamental rights of the individual to privacy and data protection, national law must provide it with a legal remedy to put those objections before a national court which may be required to make a reference for a preliminary ruling to the Court of Justice ([347]).

6. MONITORING, SUSPENSION, REPEAL OR AMENDMENT OF THIS DECISION

(231) According to the case law of the Court of Justice ([348]), and as recognised in Article 45(4) of Regulation (EU) 2016/679, the Commission should continuously monitor relevant developments in the third country after the adoption of an adequacy decision in order to assess whether the third country still ensures an essentially equivalent level of protection. Such a check is required, in any event, when the Commission receives information giving rise to a justified doubt in that respect.

(232) Therefore, the Commission should on an ongoing basis monitor the situation in Brazil as regards the legal framework and actual practice for the processing of personal data as assessed in this Decision. In that respect, special attention should be paid to the application in practice of the requirements for data protection impact assessment; the transparency requirements and their possible limitation concerning the rights to information and access; the rules on data breaches notification; the sanction regime as well as to compliance with the limitations and safeguards with respect to government access, taking into consideration any relevant developments in that regard.

([347]) Schrems I, paragraph 65: 'It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity'.

([348]) Schrems I, paragraph 76.

(233) To facilitate the monitoring process, the Brazilian authorities, including the ANPD, are invited to inform the Commission of material developments relevant to this Decision, as regards the processing of personal data by business operators and public authorities, as well as the limitations and safeguards applicable to access to personal data by public authorities.

(234) Moreover, in order to allow the Commission to effectively carry out its monitoring function, the Member States should inform the Commission about any relevant action undertaken by the national data protection authorities, in particular regarding queries or complaints by EU data subjects concerning the transfer of personal data from the European Union to data controllers and processors in Brazil. The Commission should also be informed about any indications that the actions of the Brazilian public authorities responsible for the prevention, investigation, detection, or prosecution of criminal offences, or for national security, including any oversight bodies, do not ensure the required level of protection.

(235) In application of Article 45(3) of Regulation (EU) 2016/679 ([349]), and in light of the fact that the level of protection afforded by the Brazilian legal order may be liable to change, the Commission, following the adoption of this Decision, should periodically review whether the findings relating to the adequacy of the level of protection ensured by Brazil are still factually and legally justified.

(236) To this end, this Decision should be subject to a first review within four years after its entry into force. Periodic subsequent reviews should take place at least every four years ([350]). The reviews should cover all aspects of the functioning of this Decision, including the cooperation of the ANPD with EU data protection authorities on complaints from individuals. It should also cover the effectiveness of oversight and enforcement, in the area of criminal law enforcement and national security.

(237) To perform the review, the Commission should meet with the ANPD, accompanied, where appropriate, by other Brazilian authorities responsible for government access, including relevant oversight bodies. The participation in this meeting should be open to representatives of the members of the European Data Protection Board. In the framework of the review, the Commission should request the ANPD to provide comprehensive information on all aspects relevant for the adequacy finding, including on the limitations and safeguards concerning government access. The Commission should also seek explanations on any information relevant for this Decision that it has received, including public reports by Brazilian authorities or other stakeholders in Brazil, the European Data Protection Board, individual data protection authorities, civil society groups, media reports, or any other available source of information.

(238) On the basis of the review, the Commission should prepare a public report to be submitted to the European Parliament and the Council.

(239) Where available information, in particular information resulting from the monitoring of this Decision or provided by Brazilian or Member States' authorities, reveals that the level of protection afforded by Brazil may no longer be adequate, the Commission should inform the competent Brazilian authorities thereof and request that appropriate measures be taken within a specified, reasonable timeframe.

(240) If, at the expiry of that specified timeframe, the competent Brazilian authorities fail to take those measure or otherwise demonstrate satisfactorily that this Decision continues to be based on an adequate level of protection, the Commission will initiate the procedure referred to in Article 93(2) of Regulation (EU) 2016/679 with a view to partially or completely suspend or repeal this Decision.

(241) Alternatively, the Commission will initiate this procedure with a view to amend the Decision, in particular by subjecting data transfers to additional conditions or by limiting the scope of the adequacy finding only to data transfers for which an adequate level of protection continues to be ensured.

([349]) According to Article 45(3) Regulation (EU) 2016/679, '[t]he implementing act shall provide for a mechanism for a periodic review, […] which shall take into account all relevant developments in the third country or international organisation'.

([350]) Article 45(3) Regulation (EU) 2016/679 provides that a periodic review must take place 'at least every four years'. See also EDPB, Adequacy Referential, WP 254 rev. 01.

(242) The Commission should also consider initiating the procedure leading to the amendment, suspension, or repeal of this Decision if, in the context of the review or otherwise, the competent Brazilian authorities fail to provide the information or clarifications necessary for the assessment of the level of protection afforded to personal data transferred from the European Union to Brazil, or as regards compliance with this Decision. In this respect, the Commission should take into account the extent to which the relevant information can be obtained from other sources.

(243) On duly justified imperative grounds of urgency, the Commission will make use of the possibility to adopt, in accordance with the procedure referred to in Article 93(3) of Regulation (EU) 2016/679, immediately applicable implementing acts suspending, repealing, or amending the Decision.

7. **FINAL CONSIDERATIONS**

(244) The European Data Protection Board published its opinion ([351]), which has been taken into consideration in the preparation of this Decision.

(245) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93(1) Regulation (EU) 2016/679,

HAS ADOPTED THIS DECISION:

Article 1

For the purpose of Article 45 of Regulation (EU) 2016/679, Brazil ensures an adequate level of protection for personal data transferred from the European Union to controllers and processors in Brazil subject to the General Data Protection Law (LGPD).

Article 2

Whenever the competent authorities in Member States, in order to protect individuals with regard to the processing of their personal data, exercise their powers pursuant to Article 58 of Regulation (EU) 2016/679 with respect to data transfers falling within the scope of application set out in Article 1, the Member State concerned shall inform the Commission without delay.

Article 3

1. The Commission shall continuously monitor the application of the legal framework upon which this Decision is based with a view to assessing whether Brazil continues to ensure an adequate level of protection within the meaning of Article 1.

2. The Member States and the Commission shall inform each other of cases where the Brazilian Data Protection Authority (Agência Nacional de Proteção de Dados – ANPD), or any other competent Brazilian authority, fails to ensure compliance with the legal framework upon which this Decision is based.

3. The Member States and the Commission shall inform each other of any indications that interferences by Brazilian public authorities with the right of individuals to the protection of their personal data go beyond what is strictly necessary, or that there is no effective legal protection against such interferences.

4. After four years from the date of the notification of this Decision to the Member States and subsequently at least every four years, the Commission shall evaluate the finding in Article 1 on the basis of all available information, including the information received as part of the review carried out together with the relevant Brazilian authorities.

([351]) European Data Protection Board, opinion on an adequacy decision concerning Brazil, November 2025. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282025-regarding-european-commission-draft_en.

5. Where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the competent Brazilian authorities and may suspend, repeal, or amend this Decision.

6. The Commission may also suspend, repeal, or amend this Decision if the lack of cooperation of the Brazilian government prevents the Commission from determining whether the finding in Article 1 of this Decision is affected.

Article 4

This Decision is addressed to the Member States.

Done at Brussels, 26 January 2026.

For the Commission
Michael McGRATH
Member of the Commission