Opinion 28/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by Brazil

Version 1.0

Adopted on 04 November 2025

ADOPTED

Executive summary

On 5 September 2025, the European Commission started the process towards the adoption of its draft implementing decision ('Draft Decision') on the adequate protection of personal data by the Federative Republic of Brazil ('Brazil').

On 5 September 2025, the European Commission asked for the opinion of the European Data Protection Board ('EDPB'). The EDPB's assessment of the adequacy of the level of protection afforded by Brazil has been made on the basis of the examination of the Draft Decision itself as well as on the basis of an analysis of the documentation that is publicly available in the official websites of the Brazilian authorities.

The EDPB focused on the assessment of both the general GDPR[1] aspects of the Draft decision and on the access by public authorities to personal data transferred from the EEA for the purposes of law enforcement and national security, including the legal remedies available to individuals in the EEA. The EDPB also assessed whether the safeguards provided under the legal framework in Brazil are in place and effective.

The EDPB has used as main reference for this work the Adequacy Referential adopted on 28 November 2017 by the Article 29 Working Party[2] as last revised and adopted on 6 February 2018 by the EDPB ('Adequacy Referential') and the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

The EDPB positively notes that the data protection framework, in particular, General Data Protection Law in Brazil ('LGPD'), together with Presidential decrees and binding regulations issued by Brazil's Data Protection Authority (Agencia Nacional de Proteção de Dados, 'ANPD'), establish requirements (including in relation to the principles, data subject rights, transfers, oversight and redress) that are closely aligned with the GDPR and case law of the Court of Justice of the European Union ('CJEU').

The EDPB also concluded that the European Commission should clarify in the Draft decision certain aspects of Brazil's legal framework and closely monitor its developments.

In relation to the accountability principle and the requirements for the data protection impact assessment, the EDPB considers important the obligation to conduct it in cases where the processing could result in high risk to the rights and freedoms of natural persons and that the DPIA covers the assessment of necessity and proportionality of the processing. Therefore, the EDPB invites the European Commission to monitor the practical implementation of these requirements.

The LGPD foresees a limitation to the provision of information to the data subjects or the supervisory authority on the basis of the 'commercial and industrial secrecy' in certain instances. Taking into account the importance of transparency requirements for the data subjects' possibility to control how their data are processed, as well as the importance of

[1] Regulation 2016/679/EU 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.
[2] Article 29 Working Party, WP 254 rev.01, adopted on 28 November 2017 and as last revised and adopted on 6 February 2018, endorsed by the EDPB

the obligations to cooperate with the supervisory authority, in particular, to provide information necessary for its supervisory tasks, the EDPB invites the European Commission to monitor the implementation of these limitations in practice to better understand its impact on the rights of information and access, as well as, on powers of the ANPD, if any.

In relation to the onward transfer rules, the EDPB invites the European Commission to clarify in the Draft decision whether transfers can be carried out in accordance with conditions, equivalent to Article 49 of the GDPR, only in the exceptional circumstances where other instruments for transfer cannot be used. The Commission is also invited to clarify whether the data subjects are informed on: possible risks of the transfer when this is based on their consent and on circumstances of the transfer (duration and purpose of transfer, the destination countries, responsibilities of the parties involved, data subjects' rights and means to exercise them) irrespective of the transfer tool used.

Furthermore, the EDPB invites the European Commission to elaborate further on the tasks of the National Council for Personal Data and Privacy Protection Council and its interaction with the ANPD.

In relation to access and use by Brazilian public authorities of personal data transferred to controllers and processors in Brazil for criminal law enforcement and national security purposes ('government access'), the EDPB notes the LGPD does not apply to data processing conducted for the *exclusive* purposes of public safety, national defence, State security, or the investigation and prosecution of criminal offenses. At the same time, the EDPB positively notes that the Federal Supreme Court of Brazil in its case-law has interpreted the LGPD in a way that expanded its partial applicability to the processing of personal data for criminal investigations and maintenance of public order.

In light of this, it invites the Commission to further assess and clarify in the draft Decision the applicability of the LGPD in case of personal data processing for criminal law enforcement purposes, including ANPD's investigatory and corrective powers vis-a-vis law enforcement authorities, as well as to take into careful consideration any relevant development in this regard as part of its monitoring obligation.

Being mindful of the fact that States are granted a broad margin of discretion in defining matters of national security, which then allows for national security exemptions in the processing of personal data, the EDPB invites the Commission to describe and explain more precisely in the draft Decision the outline of the concept of national security under Brazilian law. Related to this, the EDPB invites the Commission to further clarify how exemptions from the LGPD for national security purposes relate to the collection and sharing of data between the public entities within the Brazilian Intelligence system (SISBIN).

Table of Contents

1. INTRODUCTION 5

2. GENERAL DATA PROTECTION ASPECTS 6

2.1 Accountability and data governance 6

2.2 Scope and definitions 7

2.2.1 Material and territorial scope of the LGPD 7

2.2.2 Definitions 7

2.3 Data protection principles and legal bases 8

2.3.1 Principles of the processing 8

2.3.2 Security measures and breaches 9

2.3.3 Lawfulness of processing 10

2.4 Individual rights 11

2.5 Restrictions on onward transfers 11

2.6 Procedural and enforcement mechanisms 13

2.6.1 Independent oversight 13

2.6.2 Redress 14

2.6.3 Sanctions 14

3. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN BRAZIL 15

3.1 Access and use by Brazilian public authorities for criminal law enforcement purposes 15

3.1.1 Legal framework in the areas of criminal law enforcement 15

3.1.2 Necessity and proportionality 17

3.1.3 Further use of data and onward transfers 18

3.1.4 Oversight and Redress 19

3.2 Access and use by Brazilian public authorities for national security purposes 20

3.2.1 Scope of the exemption of art. 4 (III) LGPD and its applicability to criminal offenses against state security 20

3.2.2 Legal Framework for national security 21

3.2.3 Onward transfers and international agreements 23

3.2.4 Oversight and Redress 23

4. IMPLEMENTATION AND MONITORING OF THE DRAFT DECISION 24

The European Data Protection Board

Having regard to Article 70(1)(s) of the Regulation 2016/679/EU 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 (hereinafter GDPR),

Having regard to the European Economic Area Agreement (EEA) and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[3],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION:

[3] References to 'Member States' made throughout this opinion should be understood as references to 'EEA Member States'.

1. INTRODUCTION

(1) Chapter V of the GDPR sets out conditions for transfers of personal data to a third country or to an international organisation. Transfers of personal data may take place on the basis of an adequacy decision by the European Commission (Article 45 GDPR) or, in the absence of such an adequacy decision, where the controller or processor provides appropriate safeguards, including enforceable rights and legal remedies for the data subject (Article 46 GDPR). In the absence of either an adequacy decision or appropriate safeguards, a transfer or set of transfers to a third country or an international organisation shall take place only under certain conditions (Article 49 GDPR).

(2) The EDPB recalls that adequacy decisions recognise the continuous protection of personal data transferred from the EEA to third countries or international organisations and are a robust transfer tool to ensure the data subject's rights are safeguarded when data are transferred outside the EEA. According to the Adequacy Referential[4], and to the relevant case-law of the CJEU[5], while the third country does not have to provide a level of protection identical to that guaranteed in the EU legal order, the expression 'adequate level of protection' in Article 45(1) of the GDPR must be understood as requiring that third country actually ensures, by reason of its domestic legislation or its international commitments, a level of protection of fundamental rights and freedoms essentially equivalent to that guaranteed within the European Union, read in the light of the Charter of Fundamental Rights.

(3) Brazil is a Federative Republic composed of the union of the 26 States and one Federal District, as established in its Federal Constitution ('Constitution')[6]. Brazilian States also have their own constitutions, which must not contradict the Federal Constitution. Privacy and data protection are protected in the Constitution as fundamental rights (Articles 5(X), 5(XII) and 5(LXXIX) of the Constitution)[7] and recognised by the Constitutional court for any person, including a foreigner, irrespectively whether such person is resident in Brazil[8] or not.

(4) The main piece of legislation governing data protection is the General Data Protection Law or 'Lei Geral de Proteção de Dados ('LGPD') (No 13.709 of 14 August 2018, last amended by the law No. 14.460 of 25 October 2022). The LGPD is supplemented by the binding decrees (Presidential Decree No. 10.474 of 26 August 2020 and Presidential Decree No. 11.758 of 30 October 2023), which are legally binding and enforceable[9].

(5) In addition to LGPD, the Brazilian data protection framework includes binding regulations issued by Brazil's Data Protection Authority (Agencia Nacional de Proteção de Dados, 'ANPD')[10]. These regulations provide further rules on the interpretation and application of the LGPD[11]. For example, Regulation No. 4 of 24 February 2024 on the Application of Administrative Sanctions, Regulation No. 15 of 24 April 2024 on Security Incidents Notification ('Regulation on Security Incidents Notifications'), Regulation No. 19 of 23 August 2024 on

[4] Article 29 Working Party, WP 254 rev.01, adopted on 28 November 2017 and as last revised and adopted on 6 February 2018, endorsed by the EDPB, Chapter 3, C.
[5] CJEU, October 6, 2015, Judgment in case C-362/14, Maximillian Schrems v Data Protection Commissioner ('Schrems') and General Court, September 3, 2025, Judgment in case T-553/23, Philippe Latombe v European Commission ('Latombe').
[6] See Recital 7 of the Draft decision.
[7] See Recital 8 of the Draft decision.
[8] See Recital 9 of the Draft decision.
[9] See Recitals 11 and 12 of the Draft decision.
[10] All binding regulations issued by the ANPD can be found here: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd.
[11] See Recital 13 of the Draft decision.

International Transfer of Personal Data ('Data Transfer Regulation'), Regulation No. 2 of 27 January 2022 on the Application of the LGPD to Small and Medium Enterprises, Regulation No. 18 of 15 July 2024 on the Role of the Data Protection Officer ('DPO Regulation').

(6) The EDPB welcomes the constitutional recognition of the rights to privacy and to data protection as fundamental rights, further implemented via national law. In addition, the EDPB positively notes the international commitments Brazil has entered into[12]

(7) The EDPB notes that pursuant to Articles 47 and 94 of Regulation (EU) 2018/1725, European Union institutions[13], bodies, offices and agencies may transfer personal data to a third country, territory, sector, or international organisation recognised by the European Commission under Article 45(3) Regulation (EU) 2016/679 as ensuring an adequate level of protection, provided the transfer solely serves tasks within the controller's competence, without requiring further authorization. The EDPB invites the European Commission to recall this legal possibility in the recitals of the Draft Decision.

2. GENERAL DATA PROTECTION ASPECTS

2.1 Accountability and data governance

(8) The LGPD provides for the accountability principle as one of the general principles applicable to processing of personal data. According to it, controllers and processors[14] shall adopt appropriate technical and organizational measures to effectively comply with their data protection obligations and they have to be able to demonstrate such compliance, among other to the competent supervisory authority (Article 46 LGPD). The EDPB notes that such measures include the designation of a Data Protection Officer (Article 41 LGPD) as further detailed in the ANPD's DPO Regulation; the Data Protection Impact Assessment (Article 38 LGP) as well as the keeping of records of data processing activities (Article 37 LGPD). Furthermore, the LGPD states that controllers and processors may formulate internal rules for good practice and governance models including plans for educational activities, internal supervision mechanism and risk mitigation (Article 50 LGPD). The EDPB positively notes that such instruments are similar to those foreseen in the GDPR to implement the accountability principle and welcomes such close alignment.

(9) The EDPB notes that with regards to the DPIA, the LGPD does not include clear obligation to conduct the DPIA in cases where the processing could result in high risk to the rights and freedoms of natural persons, where it only refers to the possible request by the ANPD. In this regard, the EDPB notes that the ANPD recommends to conduct DPIA when processing operation may result in high risk in the 'Frequently asked questions'[15] relating to the DPIA ('FAQs on DPIA'). Additionally, the LGPD does not explicitly include the assessment of the necessity and proportionality within the scope of the DPIA. However, the FAQs on DPIA

[12] See Recitals from 8 to 10 of the Draft Decision.
[13] Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR'), OJ L 295, 21.11.2018, p. 39.
[14] Processing agents, according to Article 5(IX) LGPD.
[15] https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

recommend controllers and processors to assess in their DPIAs the necessity and proportionality of the processing.

(10) Against this background, the EDPB invites the European Commission to monitor the practical implementation of these requirements to verify that the DPIA is conducted when processing operation can result in high risk to the rights and freedoms of natural persons and that the assessment of the necessity and proportionality of the processing operations in relation to the purposes is also included in the DPIAs.

2.2 Scope and definitions

(11) Chapter 3 of the Adequacy Referential is dedicated to the 'Content Principles' and refers to basic data protection concepts and principles. A system of a third country or international organisation must contain such basic concepts and principles to ensure an essentially equivalent level of protection of personal data to the one guaranteed by EU law. They do not have to mirror the GDPR terminology but should reflect and be consistent with the concepts enshrined in EU data protection law. The Adequacy Referential refers to the following important concepts: 'personal data', 'processing', 'data controllers', 'data processor', 'recipient', and 'sensitive data'. This aspect of the Brazilian law will be commented in the next paragraphs.

2.2.1 Material and territorial scope of the LGPD

(12) The EDPB welcomes that the LGPD's scope of application, both material and territorial is very similar to the one foreseen by the EU data protection framework.

(13) Article 4 of the LGPD excludes from its scope processing for purely personal and non-economic purposes and such exceptions is also envisaged in the GDPR (Article 2(2)(c) GDPR). Additionally, some other processing operations fall partially outside of the scope of the LGPD, notably, processing for: public safety, national defense, state statutory, or the investigation and prosecution of criminal offenses; journalistic and artistic purposes; academic research; health research (Article 3(III) LGPD). This is further detailed in Section 3.1 of this Opinion.

(14) With specific regard to the partial application of the LGPD to the processing of personal data carried out for journalistic and artistic purposes, the EDPB notes that the scope of the exception is equivalent to the one set in Article 85 (2) of the GDPR[16], i. e. such exception applies only when personal data is processed exclusively for such purpose, all other processing by press, media, artistic bodies fall within the scope of the LGPD. Also, some exceptions envisaged for the processing of the personal data for exclusively for academic purposes, i.e. Articles 7 (requirements for legal basis) and 11 (rules on the processing of sensitive data) of the LGPD remains applicable[17]. The scope of these exceptions is also in line with the one set in Article 85(2) of the GDPR.

2.2.2 Definitions

(15) The EDPB positively notes the alignment with the EU data protection framework in relation to the definitions used in the LGPD which are consistent with the ones envisaged in the GPDR.

[16] See also Recital 35 of the Draft decision.
[17] See also Recital 32 and 33 of the Draft decision.

In particular, the LGPD defines 'personal data', 'pseudonymous information', 'anonymous data'[18], 'data processing', 'data controller', 'data processor' and 'sensitive data' (Article 5 LGPD) in a similar manner as they are defined in the GDPR, namely Recital 26, Articles 4 and 9(1). Other definitions, e.g. 'data subject', 'data protection officer', 'consent', 'data protection impact assessment' and a concept of 'joint controllership'[19] are also essentially equivalent to the concepts as foreseen in the GDPR.

2.3 Data protection principles and legal bases

2.3.1 Principles of the processing

(16) The Adequacy Referential, in accordance with the GDPR, establishes that data must be processed in a lawful, fair, and legitimate manner. Pursuant to Article 6 of the LGDP, activities of processing of personal data shall be done in good faith and be subject to the following principles: purpose, adequacy, necessity, free access[20], data quality, transparency, security, prevention, non-discrimination, liability and accountability.

(17) Taking into consideration the concepts of these principles, the Brazilian legal system enshrines the same data processing principles set out in Article 5 of the GDPR. For example, in relation to the purpose limitation, the LGPD provides in Article 7, Paragraph 7, that 'the subsequent processing of personal data referred to in paragraphs 3 (publicly accessible personal data) and 4 (data manifestly made public by the data subject) of this article may be carried out for new purposes, provided that legitimate and specific purposes for the new processing and the preservation of the rights of the data subject are observed, as well as the grounds and principles set forth in this Law'.

(18) The GPDR clearly requires that such subsequent processing would take place only if such new purpose is compatible with initial purpose. The requirement to ensure compatibility of purposes (as well as compliance with applicable ethical standards and technical and legal safeguards) is highlighted in the Guide for processing personal data for academic purposes and for conducting studies and research issued by the ANPD, as well as in the Guidelines on the legitimate interest. The ANPD in the guidelines on the Legitimate Interest explains how the data controller must demonstrate an effective link between the two purposes of processing and consider the 'legitimate expectations' of the data subject. These guidelines further clarify that 'The analysis of legitimate expectations may be based on several factors, among which the following may be highlighted: d) the intended purpose of the data collection and its compatibility with processing based on legitimate interest'. The EDPB welcomes such clarification by the ANPD, which help to better align the requirements of the purpose limitation.

(19) The principle of storage limitation provided in the GDPR stipulates that data shall only be stored for the period necessary to ensure the purposes for which it is processed (Article 5(1)(e) GDPR). Even though Article 6 of the LGPD does not explicitly includes storage limitation principle, this article should be read together with the Article 15 of the LGPD that specifies the requirement in case of termination of the data processing. In this article storage limitation principle is clearly linked with the 'adequacy' and 'necessity' principles that are within general

[18] Article 12 of the LGPD further details that anonymized data are not considered to be personal data except when the anonymization has been or can be reversed through reasonable efforts. This Article explains that 'reasonable' should be considered taking 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.
[19] See Article 42, paragraph 1(I), of the LGPD.
[20] 'Free access: guarantee to the data subjects of facilitated and free of charge consultation on the form and duration of the processing, as well as on the integrity of their personal data' (Article 6, part IV, LGPD).

principles listed in Article 6 of the LGPD. For the better clarity, the EDPB encourages the European Commission to clarify in the Draft decision interaction of Articles 6 and 15 of the LGPD in relation to storage limitation principle.

(20) Additionally, regarding the storage limitation requirements, Article 16 of the LGPD establishes the conditions for storage and erasure of personal data after the end of the processing. This Article also foresees four purposes for which data can be kept after the end of data processing: (1) for compliance with legal or regulatory obligations; (2) research purposes, ensuring, where 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. The EDPB notes that these processing situations are in line with the storage limitation principle enshrined in the GDPR.

(21) The transparency and fairness principle strives to ensure that the data subjects have control over their personal data and, for this purpose, information shall be provided to the data subject in a proactive manner as a rule[21]. Meanwhile the LGPD establishes a limitation to this principle when it comes to 'commercial and industrial secrecy' which may have an impact for the data subjects to receive information on their data processing in order to be able to exercise their control over it (e. g. via submission of the complaint to the ANPD). However, the European Commission in the Draft decision explains that this limitation should be interpreted in light of Brazil's Law on Access to Information and Presidential Decree No. 7.721 of 16 May 2012 and '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'[22].

(22) In light of the importance of the transparency principle, the EDPB invites the European Commission to monitor the implementation of this provision in practice to better understand its impact on the right of information and access.

2.3.2 Security measures and breaches

(23) The LGPD includes the security and prevention principles requiring to apply measures for the protection of personal data and prevention of damages related to such processing (Article 6(VII) and (VII), LGPD), moreover, the LGPD explicitly states that where security measures are not appropriately implemented, data processing is considered to be unlawful. The law requires to implement measures necessary to demonstrate compliance with this principle by the risk-based approach (Articles 44, 46 and 47 LGPD) and follow the requirements for the breach assessment and breach notification (Articles 48 and 49 LGPD). The EDPB positively notes that such principles and obligations are closely aligned to those laid down in the GDPR.

(24) The EDPB welcomes that the adoption of additional binding Regulation on Security Incidents Notifications by the ANPD which provide the concept of the incident and details for the assessment of its severity (e. g. when the incident is considered to create risks to data subjects or significantly affect the fundamental interests and rights of the data subjects and therefore

[21] This is also stressed by the Adequacy Referential, See Chapter 3, A(7).
[22] See Recital 81 of the Draft decision.

shall be communicated to the ANPD and data subject) as well as on incident notification requirements[23]. In this regard, the EDPB notes that, according to the Regulation on Security Incident Notifications, as a general rule, 'the communication of a security incident to the ANPD must be carried out by the controller within three working days'[24], and invites the European Commission to align its Draft decision (Recital 75) accordingly [25].

(25) In relation to notification of data breaches, the EDPB notes that the LGPD states that such notification (to both the ANPD and data subject), shall include, among others, information on technical and security measures used for the protection of personal data, adopted before and after the incident, observing commercial and industrial secrets (Article 6(III) and Article 9(II LGPD). The EDPB understands the necessity to effectively ensure that the right to privacy and data protection does not adversely affect the protection of other rights and invites the Commission to monitor implementation of such limitation where information on the incident has been provided partially (taking into consideration commercial and industrial secrets), and its impact on powers of the ANPD, if any.

2.3.3 Lawfulness of processing

(26) The EDPB notes that the lawfulness principle and its implementation, as foreseen in the LGPD (Articles 5(XII), 7, 8 and 10), is closely aligned with the one enshrined in the GDPR (Articles 4(11), 6, 7 and 9) and welcomes this alignment.

2.3.3.1 Legitimate interest

(27) The requirements of the legitimate interest to be used as a legal basis for the processing in the LGPD (Articles 7(IX)) are aligned with the GDPR (Articles 6(1)(f)). The LGPD also stresses that fundamental rights and liberties (which includes the right to data protection[26]) should usually prevail.

(28) The EDPB notes that Article 10 LGPD lists legitimate purposes for which such legal basis could be used. One of these legitimate purposes is to support and promote the controller's activity (Article 10(I) LGPD).

(29) While this expression seems to be broad, the EDPB notes that the conditions for the 'legitimate interest' to be used are further detailed in the Guide 'Legal bases for the processing of personal data – Legitimate Interest' ('Legitimate interest guide') adopted by the ANPD. This guide clarifies that for an interest to be considered 'legitimate', three conditions shall 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[27]. These conditions are similar to three cumulative conditions for the processing of personal data to be lawful under this legal basis, specified by the CJEU[28], and their further explanation provided by the Court. Furthermore, the conditions for the 'legitimate interest' specified in the Legitimate interest

[23] See Recitals from 73 to 77 of the Draft Decision.
[24] See Article 6 and 9 of the Regulation on Security Incident Notifications.
[25] See Recital 75 of the Draft Decision according to which 'Notification of a security incident to the ANPD and the data subjects shall take place within three days (72 hours) of the controller becoming aware of it'.
[26] See Paragraph 3 of this opinion.
[27] See Recital 52 of the Draft decision
[28] For example, CJEU, December 7, 2023, Judgment in Joined Cases C-26/22 and C-64/22, SCHUFA Holding AG, paragraph from 75 to 80.

guide are close to the ones of the Guidelines adopted by the EDPB[29]. The EDPB welcomes approach taken by the ANPD in regard to legitimate interest and its usage for the processing.

2.4 Individual rights

(30) The EDPB welcomes that the LGPD provides individuals with the similar rights as those laid down in the GDPR (both in Chapter III). In particular the LGPD envisages the right of access, the right to rectification, the right to portability of data, the right to restriction of the processing, the right to erasure, the right to information, the right to deny or withdraw the consent, and the right to object the processing and the right to petition (Articles 9 and 18 LGPD).

(31) The LGPD also provides data subjects with the right to request the review of decisions made solely based on automated processing of personal data that affect his/her interests (Article 20 LGPD). The content of Article 20 of the LGPD in substance mirrors Article 22 of the GDPR.

(32) The EDPB notes that, in relation to the data subject rights, the Brazilian Habeas Data Law establishes specific provisions to grant the right to access and the right to rectification within a short timeline (10 and 15 days respectively) of an individual's request, and welcomes this aspect.

(33) The EDPD considers that LGPD sets essentially equivalent requirements for the data subject rights as those ensured in the GDPR.

2.5 Restrictions on onward transfers

(34) The Adequacy Referential clarifies that the level of protection of natural persons whose personal data is transferred under an adequacy decision must not be undermined by the onward transfer and therefore any onward transfer 'should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller'.

(35) In relation to adequacy assessment of the Brazil's legal framework and practice, onward transfer means the transfer of personal data from the entity, acting as a Controller, within the territorial scope of LGPD Brazil, to the entity outside this scope.

(36) The requirements on the onward transfer are laid down in the Chapter V of the LGPD and further complemented by the ANPD via the adoption of the 'Data Transfer Regulation' which provides the definitions of 'transfer', 'international data transfer', 'importer', 'exporter' and include detailed requirements for transfers.

(37) The EDPB positively notes that the definition of 'transfer' and of 'international data transfer' are aligned with those of the EDPB guidelines 05/2021[30].

(38) According to the LGPD and the Data Transfer Regulation, onward transfers can only take place for legitimate, specific and explicit purposes and when specific instruments or conditions are in place (Article 33 LGPD and Articles from 9 to 33 Data Transfer Regulation)[31]. The EDPB appreciate that these instruments are close to the transfer tools foreseen in Chapter V GDPR.

[29] Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR (Version 1.0), adopted on 8 October 2024.
[30] Par. 9, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, adopted on 14 February 2023.
[31] See also Recitals from 101 to 109 of the Draft Decision.

However, the EDPB invites the European Commission to clarify in the Draft decision whether transfers can be carried out in accordance with Article 33 (III) to (IX) of the LGPD only in the exceptional circumstances, where conditions under Article 33 (I) to (II) of the LGPD are not met[32].

(39) However, Data Transfer Regulation specifies that international transfers of personal data are allowed 'when the data subject has provided specific and distinguishable consent for such transfer, with previous information on the international nature of the intended operation, clearly distinguishing it from other purposes'. It is not clear whether such requirement entails the obligation to inform data subjects about the possible risks of international transfers arising from the absence of adequate protection in the third country and the absence of appropriate safeguards (e. g. information that there might not be a supervisory authority and/or data processing principles and/or data subject rights in the third country) which is a requirement under Article 49(1)(a) GDPR. For the EDPB, and under the GDPR, the provision of this information is essential in order to enable the data subject to give an informed consent with full knowledge of these specific facts of the transfer. Thus, the EDPB invites the European Commission to clarify in the Draft Decision whether the data subject is informed on possible risks of such transfer arising from the absence of adequate protection in the third country and of appropriate safeguards.

(40) Moreover, the Data Transfer Regulation includes that 'Both controller and processor shall adopt effective measures capable of demonstrating observance of and compliance with personal data protection rules and the effectiveness of such measures, in a manner which is compatible with the level of risk of the processing and with the modality of international transfer used' (Article 4 Paragraph 2 Data Transfer Regulation). The EDPB welcomes the inclusion of this obligation. At the same time, it would be beneficial to clarify that the effectiveness of these measures should be assessed so as to also ensure that local legislation of relevant third country would not undermine the continuity of protection of the data subjects whose data are transferred[33]. The EDPB invites the European Commission to clarify that this element will also be taken into consideration in the transfer scenarios.

(41) The EDPB welcomes the inclusion of an explicit transparency requirement in relation to the data subject, i. e. data subjects have the right to receive the contractual instrument used for the onward transfer as well as the description of such transfer, e. g. duration and purpose of transfer, the destination countries, responsibilities of the parties involved, data subjects' rights and means to exercise them (Article 16 Data Transfer Regulation).

(42) However, it seems that such scope of the transparency obligation is relevant only when transfers are carried out on the basis of standard contractual clauses and not when other tool are used[34]. Therefore, the EDPB invites the European Commission to clarify that the same transparency obligations apply irrespective of the transfer tool used.

(43) The EDPB also notices that requirements for the content of the binding corporate rules ('BCR') are not fully in line with the ones in the GDPR, in particular Article 47(2) (f) and (l) of the GDPR. In order to ensure that the level of protection afforded by the GDPR would not be undermined,

[32] Article 49 GDPR specifies that derogations envisaged in this article can only be used in the absence of an adequacy decision pursuant to Article 45(3) GDPR, or of appropriate safeguards pursuant to Article 46 GDPR.
[33] See Latombe judgement. Also see CJEU, July 16, 2020, judgement in case C-311/18 ('Schrems II').
[34] E.g., Data Transfer Regulation includes general requirements for the transparency when the BCR is intended to be used, in particular, 'the establishment and implementation of a privacy governance program which intends to establish a relationship of trust with the data subject, by means of transparent actions which ensure mechanisms for the data subject's participation' (Article 25(V) Data Transfer Regulation) and transparency in relation to exercising of data subject's rights and right to complain (Article 26(VI) Data Transfer Regulation).

the EDPB invites the European Commission to clarify in the Draft decision that also these elements[35] would be taken into account when this transfer tool has to be used for onward transfers of personal data transferred to Brazil under the adequacy decision.

2.6 Procedural and enforcement mechanisms

(44) According to the Adequacy Referential[36], and to the relevant case-law of the CJEU[37], a data protection system essentially equivalent to the European Union model must provide for: (i) an independent authority, which should oversee and enforce data protection laws, with the power to investigate and take action without external influence. The data protection systems must ensure (ii) that data controllers and processors are accountable and aware of their responsibilities, while data subjects are informed of their rights. Effective sanctions and verification processes should be in place to ensure adherence to rules; (iii) that data controllers and processors demonstrate compliance, through measures like data protection impact assessments, records of processing activities, and the appointment of data protection officers. In addition, (iv) the data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms.

(45) In this section, the EDPB has focused its assessment on the existence of an independent authority, of an appropriate redress mechanism and of effective sanctions.

2.6.1 Independent oversight

(46) The LGPD establishes the Agencia Nacional de Proteção de Dados (ANPD) as the national supervisory authority responsible for monitoring and enforcing its provisions.

(47) The EDPB welcomes the fact that the ANPD has been granted the status of 'authority of special nature', a designation intended to ensure the autonomy needed to fully exercise the legal functions and powers conferred upon it by the LGPD, notably by revoking provisions that subordinated the functioning and financial operations of the ANPD to authorisations to be granted by the Executive.

(48) Likewise, the EDPB welcomes the changes brought on 15 September 2025 to the Brazilian legal framework according to which the ANPD is now recognized as a **regulatory agency**[38]. The EDPB understands that, therefore, one of the main changes is that the ANPD will submit its budget directly to the Ministry of Planification and Budget instead of having to submit it via the Ministry of Justice. The ANPD budget remains a separate line in the Federal State Budget. The EDPB understands that the ANPD already had independence also over its budget and finance, but by becoming a regulatory agency, its administrative process is simplified.

(49) The EDPB also welcomes the new competence of the ANPD, which recently has been designated as the authority responsible for the protection of children online[39]. The EDPB takes note that according to Chapter IX of the LGPD, the ANPD is well equipped with the necessary

[35] Liability and Cooperation with the supervisory authority (Article 47(2) (f) and (l) GDPR).
[36] See Chapter 3(C) of the Adequacy Referential.
[37] CJEU, October 6, 2015, Judgment in case C-362/14, Schrems.
[38] Provisional Measure n. 1.317/2025 available at https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

[39] Law n. 15.211/2025, regarding the protection of children and minors in digital environment, available at, https://www.in.gov.br/web/dou/-/lei-n-15.211-de-17-de-setembro-de-2025-656579619.

and available powers and missions to ensure compliance with data protection rights and promote awareness, such as investigatory and sanctioning powers (Article 55-J LGPD).

(50) In relation to the staff and budget of the ANPD, which plays a role in its independency, the EDPB positively notes the recent decision to increase the staff with more than 200 new positions[40].

(51) The EDPB observes, according to Article 55-C of the LGPD, the (now) ANPD is composed of a number of bodies[41], including the National Council for Personal Data and Privacy Protection ('Council'). The EDPB take notes of its composition, which also includes representatives of the Federal Executive Branch, the Legislative, and the Judiciary[42]. The EDPB also notes that according to Article 58-B of the LGPD, the Council is responsible, inter alia, for (i) 'proposing strategic guidelines and providing background information for the preparation of the National Policy for the Protection of Personal Data and Privacy and for ANPD's activities'; and (ii) 'recommending actions to be performed by the ANPD'.

(52) With particular regard to these tasks, the EDPB considers it important to gain a clearer understanding of how they are implemented and the extent to which the Council's proposals and recommendations influence the work of the ANPD. It therefore invites the European Commission to elaborate further on these tasks and on the interaction between the Council and the ANPD, to better assess the Council's influence on the ANPD's activities.

2.6.2 Redress

(53) The EDPB welcomes the redress mechanism foreseen by the LGPD, which also provides data subjects with the right to lodge a complaint with the ANPD, and to challenge its decision by presenting an appeal to its Board of Director. Individuals may then appeal the 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. As the difference between the instrument of appeal and the instrument of recourse does not clearly emerge from the draft decision. The EDPB invites the Commission to further clarify the functioning of these two avenues, including whether the use of recourse is only limited to refusal to handle a complaint or a rejection on substance of a complaint.

(54) Likewise, the EDPB welcomes the provision of the right to compensation for material and non-material damages, as well as of the collective redress (Article 22 LGPD).

2.6.3 Sanctions

(55) The EDPB recalls that the existence of effective and dissuasive sanctions can play an important role in ensuring respect for the data protection rules, as it is a sign of the high degree of accountability and of awareness that the system ensures. The EDPB welcomes the corrective powers the ANPD is provided with, which have been exercised in several occasions[43] and includes a range of measures such as warning, fines up to two percent (2%) of the gross revenue of the private legal entity involved, daily fines, the blocking of the personal

[40] https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.
[41] According to Article 55-C of the LGPD the ANPD is comprised of: the Board of Directors, highest governing body; the National Council for Personal Data and Privacy Protection; the Disciplinary Board Office; IV – the Ombudsman´s Office; VI - the Office of Legal Affairs, and VI - Administrative units and specialized units required for the enforcement of the provisions of the LGDP. See also Recitals from 126 to 130 of the Draft decision.
[42] See also Recital 132 of the Draft decision and Article 55-C LGPD.
[43] See ANPD, Register of sanctions: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/decisoes-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

data to related to the infringement until its regularization, the temporary suspension of the relevant data processing activities, and the erasure of the personal data concerned (Article 52 LGPD)[44]. The EDPB invites the Commission to monitor their consistent application, with particular regard to sanctions.

(56) The EDPB positively notes that the ANPD has issued a (binding) Regulation on Sanctions. This Regulation categorises sanctions into different levels using objective factors such as type and volume of data processed or the impact of data subjects rights', and provide for a methodology in calculation of fines, which is in line with the requirements of the Article 83 of the GDPR.

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

(57) Pursuant to Article 45 (2) of the GDPR, the assessment of the limitations and safeguards provided for in Brazilian law as regards access and subsequent use by Brazilian public authorities of personal data transferred to controllers and processors in Brazil for criminal law enforcement and national security purposes ('government access') is an important element of the 'essential equivalence' test, as interpreted by the CJEU.

(58) The EDPB positively notes the specific attention and the factual information provided for by the Commission on this aspect in the draft Decision[45]. Therefore, the EDPB refrains from reproducing most of the factual findings and analyses in this opinion. Instead, it assesses the interference by the Brazilian system for government access for law enforcement and national security purposes on the basis of the 4 elements identified by the EDPB in the European Essential Guarantees for surveillance measures, adopted on 10 November 2020[46]:

- Guarantee A - Clear, precise and accessible legal rules;
- Guarantee B - Necessity and proportionality with regard to the legitimate objectives pursued;
- Guarantee C - Independent oversight mechanism;
- Guarantee D - Effective remedies and redress mechanisms available to the individual.

3.1 Access and use by Brazilian public authorities for criminal law enforcement purposes

3.1.1 Legal framework in the areas of criminal law enforcement

[44] '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' (Recital 135 of the Draft decision).
[45] See Recitals from 152 to 217 of the draft Decision.
[46] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

(59) The EDPB notes that access and subsequent use of personal data by Brazilian law enforcement authorities[47] is regulated by a system of legal acts of different legal nature. Data protection and privacy, including secrecy of correspondence and communications, are enshrined in Article 5 of the Constitution as fundamental rights. The EDPB particularly welcomes that the scope of the protection of such rights, similarly to the EU, is not limited to Brazilian citizens only but encompasses also foreigners residing in Brazil or not[48].

(60) Next, there are several specialised sectoral laws that govern the possible access to personal data for law enforcement purposes. As regards such access to data transferred to Brazil from the EU, particularly relevant are the Penal Code, the Telephonic Interception Law, the Civil Framework for the Internet, the Law on the Confidentiality of Financial Institutions, the Law Related to Criminal Organisations and Criminal Investigations, and other. The EDPB notes that these legal acts are publicly accessible and could be deemed sufficiently clear to give data subjects an indication as to circumstances and the conditions under which public authorities are empowered to access their data[49].

(61) Another important source of law in Brazil is the case-law of the Federal Supreme Court of Brazil, which seems to apply a broad interpretation of the scope of the rights to privacy and data protection[50], as well as the case-law of the Inter-American Court of Human Rights responsible for the interpretation and application of the American Convention on Human Rights, ratified by Brazil in 1992[51].

(62) The EDPB observes that the scope of applicability of the LGPD in case of personal data processing for criminal law enforcement purposes is partial which may lead to legal uncertainty.

(63) As acknowledged by the Commission in the draft Decision, the LGPD does not apply to data processing conducted for the *exclusive* purposes of public safety, national defence, State security, or the investigation and prosecution of criminal offenses[52]. Pursuant to Article 4(I) and (III) of LGPD, data processing in these areas will be governed by specific legislation, which must encompass the principles, and the rights of the data subjects outlined in the LGPD. To the knowledge of the EDPB, confirmed by the Commission, Brazil has not yet adopted specific legislation regarding personal data processing in the criminal justice and law enforcement field (e.g. similar to the EU Law Enforcement Directive[53]).

(64) The EDPB positively notes that the Federal Supreme Court of Brazil in its case-law[54] has interpreted the LGPD in a way that expanded its partial applicability to the processing of personal data for criminal investigations and maintenance of public order.

(65) The EDPB welcomes that the supervisory authority of Brazil, the ANPD, fully supports this interpretation and holds that '*the absence of specific legislation does not grant broad and unrestricted authorization to security agencies to process citizens' personal data for the exclusive purposes of public security and the investigation and prosecution of criminal*

[47] See the list of authorities in Recital 165 of the draft Decision.
[48] See Recitals 8 and 9 of the draft Decision.
[49] See ECtHR judgment in Zakharov, paragraph 229.
[50] See Federal Supreme Court Decision on ADI 6649, September 2022.
[51] See Recital 10 of the draft Decision.
[52] See Recitals 30 and 31 of the draft Decision.
[53] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).
[54] See Federal Supreme Court Decision on ADI 6649, September 2022.

offences without any limits[55]. At the same time, the EDPB notes that, pursuant to Article 4(III) paragraph 3 LGPD, for some specific processing of data done exclusively for law enforcement purposes, the ANPD seems to have at the moment mainly an advisory role vis-à-vis law enforcement authorities.

(66) The EDPB invites the Commission to further assess and clarify in the draft Decision the applicability of the LGPD in case of personal data processing for criminal law enforcement purposes, including the powers of the ANPD, as well as to take into careful consideration any relevant development in this regard in its future monitoring (see also the section on oversight and redress).

3.1.2 Necessity and proportionality

(67) The EDPB positively notes that, as general rule, access to communication data, both content and metadata, as well as to other categories of protected confidential information such as banking and tax data, requires prior judicial authorisation.

(68) As regards access to communication data, the EDPB welcomes that, pursuant to the Telephonic Interception Law and the case-law of the Federal Supreme Court, such measure is considered exceptional and is subject to strict conditions aimed at ensuring its necessity and proportionality[56]. Moreover, as a preventive measure against possible abuse, Brazilian law provides that interception of communications without a judicial authorisation or for purpose not authorised by the law constitute a crime punishable by up to four years in prison[57].

(69) The strict implementation of the safeguards for access to communication data is particularly relevant given the existence in Brazil of a general data retention obligation for internet connection and online application service providers to retain connection logs for one year[58]. While the EDPB positively notes that access to the retained data is only possible subject to a judicial authorisation[59], it recalls the strict approach and the restrictions on general and indiscriminate retention of communication metadata in the EU[60] and takes positive note of the additional information provided by the Commission in relation to the absence of mass data retention in the country. The EDPB therefore encourages the Commission to pay specific attention on the legal regime and practice in Brazil concerning access to communication data during the monitoring and review of the draft Decision.

(70) The EDPB positively notes that similar safeguards apply also as regards access by law enforcement authorities to tax and banking data, i.e. requirement for prior judicial authorisation, permitted only for serious crimes, existence of criminal sanctions in case of abuse, etc.

(71) According to the draft Decision, there is an exception from the general requirement for prior judicial authorisation for access by law enforcement authorities to certain categories of personal data[61]. Pursuant to Articles 15 and 16 of the Law Related to Criminal Organisations

[55] See ANPD Technical Note No 29/2024/FIS/CGF/ANPD, addressed to the Ministry of Justice and Public Security, point 5.4.1.29, available at: SEI/ANPD - 0132350 - Nota Técnica.
[56] See Recitals 169 and 170 of the draft Decision.
[57] Ibid.
[58] See Recital 173 of the draft Decision.
[59] Ibid.
[60] For more information on data retention see EDPB statement 5/2024 on the Recommendations of the High Level Group on Access to Data for Effective Law Enforcement, available at https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf.
[61] See Recital 164 of the draft Decision.

and Criminal Investigations, a police chief and the Public Prosecutor's Office may access without judicial authorisation the registration data of an investigated person about his/her: '*personal qualification, affiliation and address maintained by the Electoral Court, telephone companies, financial institutions, internet providers and credit card administrators*'[62]. In the same vein, transport companies will allow, for a period of five years, direct and permanent access by a judge, the Public Prosecutor's Office or a police chief to the databases of reservations and travel records[63].

(72) The EDPB notes that the scope of the Law Related to Criminal Organisations and Criminal Investigations is limited to the investigation and sanctioning of organised criminal groups and terrorist organisations, which pose a significant risk for the citizens and the society and thus are capable of justifying a more serious interference with the fundamental rights to privacy and data protection[64]. At the same time, the EDPB considers that the information about these exceptions provided in Recital 164 of the draft Decision is very general and not complete. In particular, it is not clear from the information in the draft Decision whether in such case the access to personal data is subject to *ex post* judicial review of the necessity and proportionality.

(73) In view of this, the EDPB invites the Commission to further clarify and explain in the draft Decision the scope and the nature of the cases where access to data by law enforcement authorities does not require judicial authorisation as well as the applicable safeguards in the Brazilian legislation. The EDPB also considers that the Commission should pay specific attention on the application of these exceptions under Brazilian law during its monitoring of the draft Decision.

3.1.3 Further use of data and onward transfers

(74) The EDPB recalls that the level of protection afforded to personal data transferred from the EU/EEA to Brazil must not be undermined by the further use or sharing of the data with recipients in Brazil or in a third country, i.e. onward transfers should be permitted only where a continued level of protection essentially equivalent to the one provided under EU law is ensured.

(75) In this regard, the EDPB positive notes that the Federal Supreme Court of Brazil has ruled that sharing of personal data between public bodies (including when shared between law enforcement and intelligence agencies) 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'[65].

(76) Notwithstanding this important ruling by the highest court in Brazil, given the already mentioned complexity, the exact scope and modalities of the application of the LGPD to law enforcement authorities, the EDPB invites the Commission to monitor closely the developments and the practice in this area.

[62] See Article 15 of the Law related to criminal organisations and criminal investigations.
[63] See Article 16 of the Law related to criminal organisations and criminal investigations.
[64] See CJEU judgment of 6 October 2020, Joined Cases La Quadrature du Net and Others, C-511/18 and C-512/18, EU:C:2020:791, paragraphs 95-98, judgment of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, paragraphs 54, 57and 60, (judgment of 2 March 2021, Prokuratuur (Conditions of access to data relating to electronic communications), C-746/18, EU:C:2021:152, paragraph 35.
[65] See Recital 187 of the draft Decision.

(77) Concerning onward transfer of personal data to criminal law enforcement authorities in third countries, the draft Decision refers to Article 33 (III) of the LGPD, which 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.'[66] The EDPB considers this explanation as too general and invites the Commission to further elaborate in the draft Decision on the conditions and safeguards governing onward transfers.

3.1.4 Oversight and Redress

(78) The EDPB recalls that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body (e.g. an administrative authority or a parliamentary body)[67].

(79) It also notes that in the Brazilian framework, as described by the Commission, the activities of criminal law enforcement authorities are supervised by different bodies: (i) the judiciary; (ii) the ANPD, and (iii) the Public Prosecutor Office.

(80) The judicial control, as explained above in the section on Necessity and Proportionality[68], applies in relation to collection and access of personal data, notably in the form of *ex ante* review and authorisation.

(81) As regards the role of the ANPD, as already explained in section 3.1.1. of this Opinion, the draft adequacy decision recalls that according to Article 4 (III) LGPD, this law does not apply to the processing of personal data carried out *exclusively* for purposes of (i) public security; (ii) national defence; (iii) State security and (iv) investigation and prosecution of criminal offences. Furthermore, Article 4(I) states that such processing will be governed by specific legislation, which, among other things, must encompass the general principles of protection and the rights of the data subjects as outlined in the LGPD. Paragraph 3 of the same Article recognises an advisory role to the ANPD in relation to the exceptions provided in paragraph III when conducted exclusively for these purposes, notably the powers of the ANPD to issue technical opinions and recommendations, as well as to request DPIAs from the relevant controllers.

(82) In its draft Decision[69], the Commission refers to an important decision dated 15 September 2022 of the Federal Supreme Court, which indicates the applicability of general data protection principles and data subjects' rights to processing of personal data by the State for the provision of public services. This decision focuses on the 'sharing of personal data' between bodies and entities of the Public Administration and in intelligence activities, and to 'access of government agencies and entities' to Citizen's Base Registry. In relation to the enforcement role of the ANPD, the EDPB understands from additional information provided by the Commission, that the ANPD has already exercised such role over the police as well as over Ministry of Justice and Public Security. This was done on the basis of the case-law which, by extending the partial applicability of general principles and data subjects' rights to the processing carried out for law

[66] Ibid.
[67] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures Adopted on 10 November 2020, see page 12 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf
[68] See Section 3.1.2 above
[69] See Recital 187 of the draft Decision

enforcement purposes, it makes the ANPD responsible for overseeing and enforcing the law in this area too.

(83) In light of the above, the EDPB invites the Commission to further elaborate on the enforcement role of the ANPD, notably with regard to the relevant legal bases and its investigatory and corrective powers vis-a-vis law enforcement authorities and monitor closely the developments in this area.

(84) Finally, the EDPB observes that the Public Prosecutor Office has a broader competence than overseeing data protection and privacy rules and imposing sanctions for violations of fundamental rights. For instance, as already explained in Section 3.1. of this Opinion, under the Law Related to Criminal Organisations and Criminal Investigations, the Public Prosecutor's Office is one of the authorities that may access without judicial authorisation registration data of an investigated person. The EDPB therefore invites the Commission to further elaborate on and explain in the draft Decision the role and the powers of the Public Prosecutor's Office in relation to the oversight of the processing of personal data by the Brazilian law enforcement authorities.

(85) Concerning redress, the EDPB positively notes that the legal mechanisms described in the first part of this Opinion and in particular the judicial remedies available to the individuals to enforce their rights to data protection and privacy, apply also in relation to the activities of the criminal law enforcement bodies.

3.2 Access and use by Brazilian public authorities for national security purposes

3.2.1 Scope of the exemption of art. 4 (III) LGPD and its applicability to criminal offenses against state security

(86) As introduced by the Commission, Art. 4 (III) LGDP exempts 'State security' from the application of the LGPD when processing personal data, alongside with public security, national defence and activities of investigation and prosecution of criminal offenses.

(87) The EDPB notes that the Brazilian legislation on '*Seguranca Nacional*' (National Security), as laid out in Law N°14.197 of 1 September 2021 modifying the Penal Code and revoking the 1983 Law on National Security[70], expresses the Brazilian concept of national security on the basis of an exhaustive list of criminal offenses[71], which address different threats to the integrity of the Brazilian State as an institution (national sovereignty, espionage (Ar.t 350-K), crimes against the democratic institutions (Art. 359-L) et al.). The norms of Law Nº 14.197 have been established as integral part of the Brazilian Penal Code.

(88) This being said, the EDPB would expect data processing of Brazilian authorities for the prosecution of the offenses laid down in Law Nº 14.197 to be governed by the regime applicable to the access and use of Brazilian authorities for criminal law enforcement purposes as described in chapter 3.2 of the draft Decision, thus facing the same considerations on data protection as stated in chapter 3.1. of this Opinion. The EDPB therefore asks the Commission to clarify in the draft Decision whether the data processing related to the prosecution of the

[70] Law No. 14.197 of September 1st, 2021, available at https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm (02.10.2026).
[71] See Recital 200 of the draft Decision.

criminal offenses listed in Law N° 14.197 are indeed governed by the data protection regime applicable to law enforcement activities, or by another regime. If it is the latter case, the EDPB invites the Commission to further explain the data protection rules applicable to the criminal prosecution of these offenses for the purposes of national security.

3.2.2 Legal Framework for national security

(89) The codified legal framework on which the draft Decision bases its findings in its chapter on government access for 'national security purposes' consists of Law N° 14.197 from 2021, Law N° 9.883 of 7 December 1999 establishing the Brazilian Intelligence System and the related Decree N° 4.376 of 2002. The two last mentioned pieces of legislation set up the Brazilian Intelligence system (Sistema Brasileiro des Inteligência (SISBIN) and its functioning. They are followed by the binding Presidential Decree N° 8.793[72] of 2016 that defines the national intelligence policy (so-called *Política Nacional de Inteligência* (PNI), as well as the LGPD in 2018.

(90) The Presidential Decree N° 8.793 of 2016 describes the subject, the aims and the limits of PNI. Activities under this decree aim at producing and spreading knowledge to the competent authorities related to facts and situations which occur within or outside the national territory, with immediate or potential influence on decision-making process, governmental action and the safety of the society and the state intelligence. Under these circumstances, intelligence refers to the whole of information – and data - required and processed in order to support the decision-making process of the executive branch in this field.

(91) According to the legal basis of SISBIN as presented by the Commission, SISBIN and its entities have been established as the core mechanism for the implementation of the PNI and as such are charged with carrying out activities pertaining to the field of national security as well as to public safety and security and the protections of democratic institutions. As to this end, SISBIN provides for knowledge exchange and integrated planning of activities[73]. In consequence, the concept of national security in Brazil in the light of the activities of SISBIN seemingly is not limited only to the criminal offenses codified within Law N° 14.197, but might be considered an integrated part of a broader concept of national intelligence.

(92) SISBIN was initially established comprising of eighteen federal entities, among them thirteen ministries, and subsequently extended to 48 so-called agencies under Decree N°11.693 of 6 September 2023 on the organisation and functioning of SISBIN[74]. The EDPB notes that cooperation within SISBIN integrates entities beyond classical security institutions, such as the Ministry of science (Art. 4 (IV), agriculture (Art. 4(XV)) and energy (Art. 4 (XVIII) and the Federal Attorney general (Art. 4 (XIX)).

(93) Whereas Decree N° 4.376 of 2002 has required the Advisory Council of the Brazilian Intelligence System to propose general standards and procedures for the exchange of 'knowledge and communication' within SISBIN[75], Decree N° 11.693 of 2023 points at the central organ of SISBIN to produce technical tools[76] for the sharing of information data and knowledge and describes the sharing and use of data obtained by SISBIN's entities. The Commission's draft Decision however does not provide any further information of such rules

[72] See Recital 199 of the draft Decision.
[73] Presidential Decree N° 8.793, section 5, names SISBIN and the organs integrated therein, knowledge exchange within SISBIN and integrated planning of the cooperation amongst the members of SISBIN as instruments for carrying out PNI.
[74] See Recital 202 of the draft Decision.
[75] See Art. 7 (II) of Decree No 4.376.
[76] See Art 10 (XI), available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm (26.09.2025).

or legal standards issued by the central organ, e.g. when SISBIN's entities share personal data amongst them.

(94) In addition, there seem to be differences in the concepts on sensitivity of information, given that under the relevant law governing SISBIN's activities, sensitivity is related to the grade of confidentiality afforded to an information[77], and of purpose limitation when compared with the general principles of the GDPR[78].

(95) As already explained above, Art. 4(III)(a) – (c) LGPD, which was codified only after the establishment of SISBIN and the setting of a national intelligence policy, exempts data processing activities carried out exclusively for the purposes of public security, national defence and state security from the application of the LGPD, except for the established general data protection principles.

(96) As underlined by the Commission in the draft Decision, the overarching framework of the Brazilian constitution as well as Brazil's participation in the Inter-American Court of Human Rights pertain to the legal framework for government access for the purpose of national intelligence. The EDPB also acknowledges that the rulings of the Brazilian Federal Supreme Court have also played an important role in defining the legal landscape[79]. The Supreme Court's rulings so far have been a concise and relevant support for the further development of personal data protection in accordance with the Brazilian constitution. At the same time, it should be noted that the rulings of the Supreme Court do not spell out or lay down general abstract data protection rules for the processing of personal data but interpret the provisions and the principles of the Constitution and the LGPD.

(97) The EDPB is mindful of the fact that States are granted a broad margin of discretion in defining matters of national security, which then allows for national security exemptions in the processing of personal data. In this context, it recalls the definition given by the European Court of Human Rights, according to which threats to national security must be distinguishable by their nature, their seriousness, and the specific circumstances from general risks for public security or from serious criminal offenses[80].

(98) It is in the understanding of the EDPB that data processed by SISBIN's entities only profits from the exemption under Art. 4 (III) LGPD when the processing is *exclusively* carried out for the purposes of public security, national defence and state security. This seems to apply specifically to the activities of the central body of SISBIN, the Brazilian Intelligence Agency (ABIN). Consequently, unless an entity of SISBIN acts on behalf of ABIN for one of these purposes - the LGPD fully applies.

(99) The EDPB calls upon the Commission to confirm this understanding and to describe and explain more precisely in the draft Decision the outline of the concept of national security under Brazilian law, in particular in relation to the collection and sharing of data between and by entities on behalf of SISBIN's activities, and with regard to the implementation of PNI. Related to this, the EDPB invites the Commission to also clarify how exemptions from the LGPD for national security purposes relate to the exemption for national security under the GDPR.

[77] See Decree No 8.793 of 2016, Decree No 11.693, Recital 204 of the draft Decision.
[78] See Art. 6 (I) LGPD which relates to legitimate and specific purposes, while the GDPR requires lawful and specified purposes.
[79] See Recital 203 of the draft Decision.
[80] ECtHR, Big Brother Watch and others vs. The United Kingdom, 25th May, 2021, § 350.

3.2.3 Onward transfers and international agreements

(100) Art. 33 LGPD defines the preconditions for international data transfer. Art. 33 (I) and (II) LGPD lay down requirements similar to an adequacy decision or the requirements for additional safeguards under the GDPR. These requirements are waived in Art. 33 (III), (VI), (VII) LGPD, which address the cases of 'legal cooperation among intelligence', transfers replying to 'a commitment made in international cooperation agreements' and transfers 'required for enforcement of a public policy or legal attribution to public service', i.e. national security and national intelligence. This decision appears to be in line with the concept of Art. 4 (III) LGPD, which restricts the application of the LGPD to solely its principles with regard to matters of public security, national defence, and state security. Thus, it could be considered that onward transfers for national intelligence purposes should be conducted in compliance with the general principles of data protection of the LGPD, while also being subject to the provisions on international cooperation provided for in the legal acts setting up PNI and SISBIN.

(101) This being said, the EDPB acknowledges that Brazil may need and does transmit personal data to foreign intelligence services for the purpose of cooperation or aiming at implementing PNI according to the aim of preventing and identifying threats based on the above mentioned integrated concept of security.

(102) As stated before, the Commission points out the applicability of the overarching framework of the Brazilian constitution and the guarantee of Habeas Data for the protection of personal data within SISBIN, which apply also for onward transfers for the purpose of national security. The EDPB invites the Commission to further clarify the legal basis and the data protection safeguards and conditions that the ABIN and the other members of SISBIN are obliged to consider prior to disclosing personal data for national intelligence purposes to foreign partners.

(103) The EDPB also notes that the Commission did not integrate considerations on the existence of international agreements concluded between Brazil and third countries or international organisations into its adequacy assessment. As the LGPD does not provide binding legislation beyond general data protection principles, such agreements might hold specific provisions for the international transfer of personal data held by the ABIN or the other SISBIN members to third countries. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purposes of national intelligence are likely to affect the applicable data protection legal framework.

(104) The EDPB therefore invites the Commission to clarify whether such international agreements for national intelligence purposes exist and to assess their potential impact on the level of protection afforded to personal data transferred from the EEA to Brazil in relation to the primarily assessed legal framework for data processing for national intelligence purposes.

3.2.4 Oversight and Redress

(105) The draft adequacy decision presents different bodies to oversee the activities of Brazilian national security authorities, notably by (i) the Executive Brach, (ii) the Legislative Branch; (iii) the ANPD; and (iv) the Judiciary. In relation to the ANPD, the EDPB recalls the consideration and conclusions made in Section 3.1.4. of this Opinion, which remain valid also here.

(106) According to the draft decision, the Chamber of External Relations and National Defence of the Council of Government is responsible for overseeing the implementation of the Intelligence National Police, and the Institutional Security Office is responsible for coordinating the activity of federal intelligence. The EDPB notes that this control only refers to ensuring that the

objectives to be achieved by the Intelligence System and to their implementation, but does not include any investigating or sanctioning powers, and does not cover the actual processing of personal data.

(107) It is in fact for the Joint Committee for the Control of Intelligence Activities (CCAI) (Legislative Branch) to exercise control in relation to intelligence activities, encompassing its legitimacy and effectiveness. The EDPB welcomes that the CCAI's structure and powers have been strengthened, increasing transparency over its activities and allowing the body to exercise a proper control, such as conducting post hoc review, audits and controls of operations in progress. The EDPB also positively notes that the CCAI can handle data subjects' complaints as part of its competence to investigate complaints about violations of fundamental rights and guarantees.

(108) The Judiciary's competence to hear cases brought by citizens against public authorities is a positive aspect, particularly as it enables judicial oversight of activities carried out in the name of national security, ensuring compliance with, among others, constitutional rights (including the right to data protection) and the LGPD. The EDPB positively notes that the possibility of appeal is provided for via the Federal Supreme Court, and ultimately via the Inter-American Court of Human Rights.

(109) It is the EDPB's understanding that in the context of national intelligence activities, data subjects' are provided with (i) the rights as enshrined in the LGPD (as a consequence of the Federal Supreme Court decision dated 15 September 2022); (ii) the right of obtain access and rectification of personal data through the constitutional redress avenue of the Habeas Data; as well as (iii) the right to compensation for material and non-material damage.

(110) The EDPB welcomes the existence of such rights and the fact that they can be invoked through judicial and administrative mechanisms, in particular the CCAI, as well as that fact that these avenues for redress are accessible to all individuals, regardless of nationality.

4. IMPLEMENTATION AND MONITORING OF THE DRAFT DECISION

(111) Concerning the monitoring and review of the Draft Decision, the EDPB notes that according to the case law of the CJEU, 'in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted an adequacy decision pursuant to (Article 45 GDPR), to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard'[81].

(112) The EDPB notes that the review of the adequacy finding will take place at least every four years, in accordance Article 45(3) GDPR[82].

(113) The EDPB welcomes that the Draft Decision in its Recital 230 foresees the participation of the EDPB in the meeting organised between the Commission and the Brazilian authorities and dedicated to performing the review of the functioning of the adequacy decision. Concerning the practical involvement of the EDPB and its representatives in the preparation and

[81] CJEU Schrems I judgement, paragraph 76. See also Article 3(4) of the Draft decision.
[82] See Recital 229 and Article 3(4) of the Draft decision.

proceeding of the future periodic reviews, the EDPB reiterates that any relevant documentation, including correspondence, should be shared in writing with the EDPB sufficiently in advance of the reviews.

For the European Data Protection Board

The Chair

(Anu Talus)