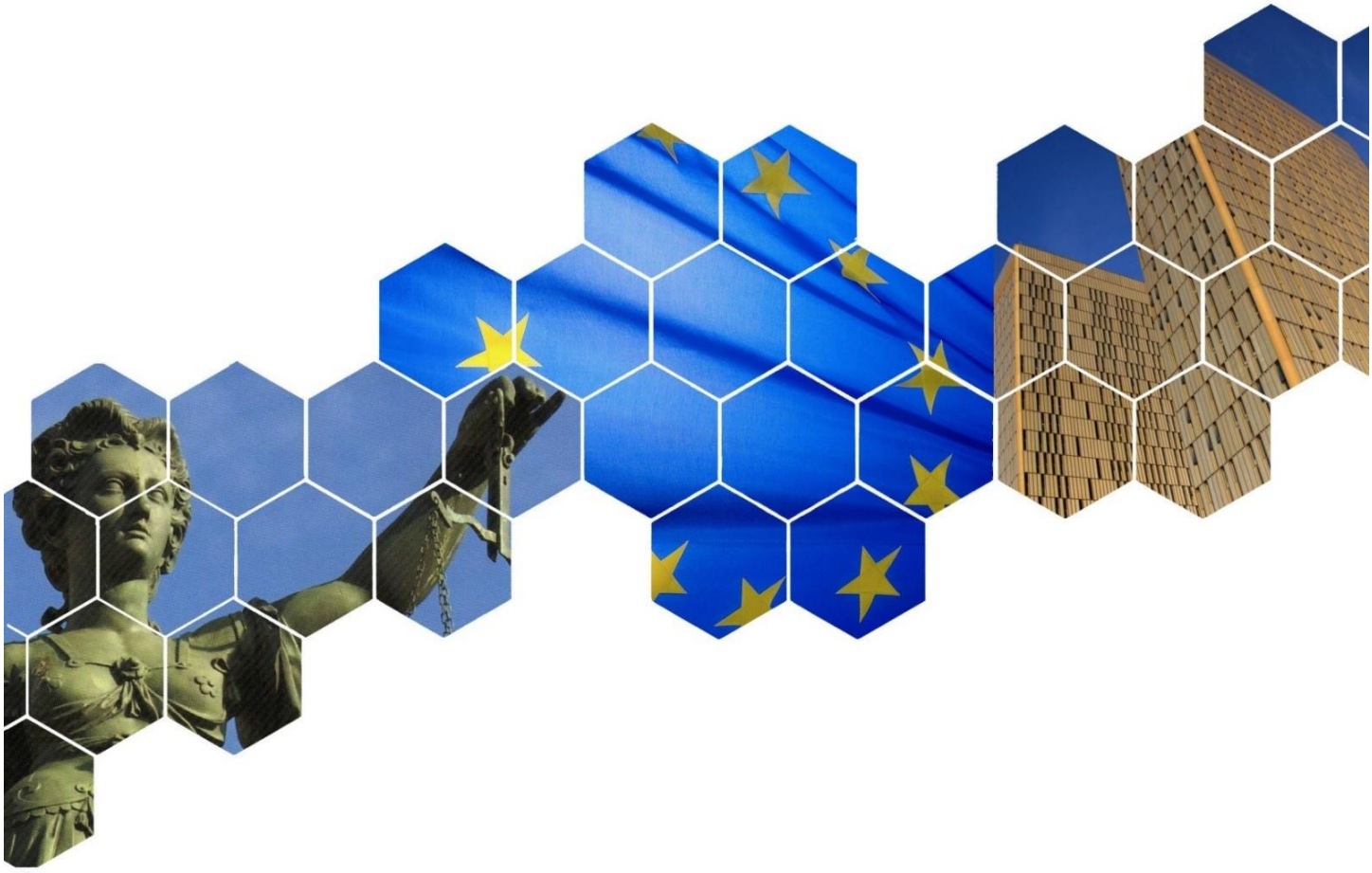
Government access to data in third countries II

Final Report

Specific Contract No. 2022-0716
Implementing the Framework Contract EDPS/2019/02



milieu
Law & Policy Consulting

KU LEUVEN

April 2023

This study has been prepared by Milieu under Contract No 2022-0716 (EDPS/2019/02) for the benefit of the EDPB.

The study has been carried out by researchers from CiTiP, KU Leuven, with the support of Milieu Consulting SRL. The authors of the study are Dr Laura Drechsler, Abdullah Elbi, Elora Fernandes, Eyup Kun, Isabela Maria Rosal, Bilgesu Sumer, and Dr Sofie Royer from CiTiP, KU Leuven.

The information and views set out in this study are those of the author(s) and do not reflect the official opinion of the EDPB. The EDPB does not guarantee the accuracy of the data included in this study. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for the use which may be made of the information contained therein.

This study does not bind the EDPB and its members in their assessment of individual data transfers. This study is not an "adequacy finding" for which the European Commission alone is competent under Regulation (EU) 2016/679 (GDPR) and Directive (EU) 2016/680 (LED).

Milieu Consulting SRL, Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: EDPB.legalstudies@milieu.be; web address: www.milieu.be.

Table of contents

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

EXECUTIVE SUMMARY

This report provides information on the legislation and practices in Mexico, and Türkiye for the situation where personal data are accessed by governmental authorities for reasons of national security or law enforcement (governmental access). This study was based on a literature review via desk research (books, journal articles, databases and other online sources), also including reports of international organisations on the country in question. The legal analysis based on the literature review and the relevant legal documents was complemented by a round of interviews with carefully selected experts with the goal of gaining insights into the practice of the analysed laws. The main findings of this approach for each country are outlined in the following paragraphs.

Mexico has a multi-layered data protection framework. Constitutionally, not only the right to data protection is guaranteed to every person, regardless of nationality, but also the data subjects' rights of access, rectification, cancellation, and opposition. Any data processing carried out by private parties in Mexico must comply with the Data Protection Law for Private Parties (LFPSSP), which the National Institute for Transparency, Access to Information, and Data Protection (INAI) oversees. For the public sector, Mexico adopted the Data Protection Law for Public Parties (LGPDSSO) in 2015. This general law establishes the main rules for data protection in the public sector while dividing competences between the 33 different federal entities in Mexico. In specific cases, such as law enforcement activities, these rules must be applied side-by-side with sector regulations. Consent is the standard legal basis for data processing by public authorities. However, the law establishes various exceptions that allow data usage without such consent. The main exception to the rules set by the LGPDSSO is data processing for national security purposes, which is regulated by the National Security Law (NSL) from 2005, which has fewer provisions on data protection. Adequate protection for individuals in situations of government access requires that different Mexican oversight authorities maintain their independent status, free from political interference.

Türkiye recognises both the right to privacy and the right to personal data protection as a fundamental right in its constitution. This protection extends to all individuals, including foreigners, and includes rights such as the right to be informed, access, rectification, and the right to be forgotten. While the Turkish Data Protection Law (TPDPL) provides secondary-level protection for personal data, it exempts judicial authorities, law enforcement, and intelligence organisations from its scope. National security and law enforcement authorities process personal data therefore without a specific legal framework, though they are still bound by any limits posed by the Constitution. Moreover, specialised laws have put in place specific safeguards and oversight mechanisms. Individuals can seek redress through *ex-post* judicial and individual complaints of violation of privacy and data protection rights before the Constitutional Court. Yet, the proportionality of governmental access can be questioned based on four concerns: (i) the necessity and proportionality of the substantial and procedural conditions for such access; (ii) the safeguards for citizens abroad and foreigners; (iii) the independence of the different oversight mechanisms; and (iv) the adequacy of the implementation of data subject rights in Turkish law.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

1 INTRODUCTION

1.1 OBJECTIVES AND SCOPE OF THE STUDY

According to Article 46 of the General Data Protection Regulation (GDPR)[1], data controllers and processors may transfer personal data to third countries or international organisations only if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Whereas it is the primary responsibility of data exporters and data importers to assess that the legislation of the country of destination enables the data importer to comply with any of the appropriate safeguards, supervisory authorities (SAs) play a key role when issuing further decisions on transfers to third countries. Hence, this report provides the European Data Protection Board (EDPB) and the SAs in the EEA/EU with information on the legislation and practice in Mexico, and Türkiye on their governments' access to personal data processed by economic operators. The report contains an overview of the relevant information in order for the SAs to assess whether and to what extent legislation and practices in the abovementioned countries imply massive and/or indiscriminate access to personal data processed by economic operators.

In order to answer the research questions, the study has

- investigated the general situation of Mexico, and Türkiye with regard to the protection of fundamental rights and freedoms, by analysing international reports and findings from public bodies (e.g. Council of Europe, UN Human Rights Council and Human Rights Committee) and renowned non-governmental bodies (e.g. Amnesty International, Human Rights Watch, Privacy International). To this end, the study also identified the countries' international commitments in the field of human rights, in particular of the right to privacy and data protection;
- analysed the legislation of the countries in order to establish the substantive and procedural conditions for government access to personal data, including law enforcement and intelligence agencies. Specific attention was paid to the authorities involved in the adoption or amendment of the related rules, and entitled to authorise the governmental access to personal information;
- investigated whether specific purposes and conditions to access personal data of foreign individuals exist in both countries;
- identified, where existing, oversight mechanisms with regard to the governmental access to personal data, and to assess the independency from the executive of the bodies empowered to perform such control; and
- focused on rights and administrative or judicial redress mechanisms that are available to data subjects (including foreign individuals) in the observed countries.

The study is not limited to an up-to-date overview of relevant legislation and case law, but also contains information with regard to the implementation of the legislation in the both countries in practice, which has mostly been collected through interviews.

1.2 LEGAL BACKGROUND

This section gives an overview of the legal framework for assessing governmental access to personal data in a third country from the perspective of EU law, where such an assessment is required in the

[1] 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).

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

context of international personal data transfers under the GDPR[2]. The main legal instruments considered are the EU-Charter of Fundamental Rights of the EU (EU-Charter), the European Convention of Human Rights (ECHR) and the GDPR[3].

1.2.1 DATA TRANSFERS IN THE GDPR

Personal data transfers to a third country or to an international organisation under the GDPR are only permitted if they comply with the requirements of Chapter V[4]. In principle, the GDPR allows the transfer of personal data to third countries or to international organisations based on three broad transfer tools, namely: (i) adequacy decisions; (ii) appropriate safeguards, i.e., legally binding and enforceable instruments between public authorities or bodies, binding corporate rules, standard contractual clauses, codes of conduct, or certification mechanisms[5]; and (iii) derogations[6]. With these tools, the GDPR intends to provide a high level of protection to personal data transferred to third countries and international organisations[7]. Accordingly, the third country, international organisation or the transfer instrument, in case of appropriate safeguards, should provide guarantees, safeguarding a level of protection essentially equivalent to that ensured within the Union[8]. The Court has gradually developed the criteria for essential equivalence in *Schrems I, Opinion 1/15, and Schrems II,* which are relevant for all transfer mechanisms provided in the GDPR[9].

1.2.2 INTERFERENCES WITH THE FUNDAMENTAL RIGHTS UNDER THE EU-CHARTER

Governmental access to personal data transferred from the EU to a third country or international organisation has been found by the CJEU to constitute an interference with Articles 7 (right to privacy), 8 (right to data protection), 21 (non-discrimination) and 47 EU-Charter (right to an effective remedy and fair trial). First, if communication data (content and/or meta-data) are maintained, accessed, and/or exposed by public authorities at the transfer's destination, this can constitute an interference with the fundamental right to privacy in Article 7[11]. Second, there can be an interference with Article 8, when the transfer of personal data constitutes processing of such data[10]. Third, due to "*the risk of data being processed contrary to Article 21 of the Charter*," the CJEU decided in *Opinion 1/15* that the transfer of special categories of personal data would require a precise and particularly solid justification[11]. Fourth, the lack of effective remedies in a third country or international organisation in a situation of

[2] Article 46 GDPR.
[3] Article 52(3) of the EU Charter states "*in so far this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.*" Therefore, the sought assessment needs to take place following the interpretation of both the CJEU and the European Court of Human Rights (ECtHR).
[4] Article 44 GDPR.
[5] Articles 46 and 47 GDPR.
[6] Article 49 GDPR.
[7] Article 44 GDPR 'to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined'.
[8] Recital 104 GDPR.
[9] Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650, paragraph 64; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 105 and 188. The *Schrems II* decision is the first to explicitly address the issue of the level of protection necessary for international data transfers under the different transfer mechanisms of the GDPR. In this case, the Court clarified the connections between the various mechanisms and ruled that they should be all afforded essentially equal levels of protection to those provided by the GDPR. See judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 92.
[10] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 124; and its paragraph 126: "*Those operations also constitute an interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the EU Charter since they constitute the processing of personal data*"; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 170 and 171; and its paragraph 83: the "*[…] the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data […]*".
[11] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 165; judgment of the Court of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 181.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

governmental access can interfere with the fundamental right to an effective remedy in Article 47[12]. However, none of the mentioned fundamental rights are absolute rights, thus where necessary, they can be limited following strict conditions listed in Article 52(1) of the EU-Charter.

According to Article 52(1) of the EU-Charter, an interference with a fundamental right can be justified, if it is (i) provided by law and (ii) respects the essence of the right, meaning that the interference must not empty the right of its core elements and prevent the exercise of the right. Furthermore, the interference must (iii) genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; and finally, (iv) it must be necessary and proportionate[13].

1.2.3 LEGALITY OF GOVERNMENTAL ACCESS

According to Article 52(1) of the EU-Charter, any interference to a fundamental right of the EU Charter must be **provided for by law**. The CJEU holds that "*the legal basis which permits the interference […] must itself define the scope of the limitation on the exercise of the right concerned*"[14]. The national laws permitting the interference shall lay down clear and precise rules governing the scope and application of the limitation[15]. As dissected in its elements below, the quality of law requirement is the first step when assessing if the interference is compatible with the EU-Charter[16].

First, the law authorising the interference, e.g., the governmental access, must be "*accessible to the persons concerned and foreseeable as to its effects*"[17]. Foreseeability refers to the formulation of the law with sufficient precision to enable persons to regulate their conduct[18]. The level of such precision depends on the particular subject-matter[19]. For example, in the particular context of secret measures of surveillance, such as interception of communications, foreseeability cannot mean that individuals should be able to foresee when the authorities are likely to intercept their communications so that they can adapt their conduct accordingly[20]. However, when executed secretly, the power granted to such secret activities may risk arbitrariness[21].

In *Schrems II*, when assessing the US surveillance programme, the CJEU stated that "[…] *the legislation*

[12] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 227. Although in this case, the interference with the PNR agreement was not found to be in violation with Article 47. See further judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 186.
[13] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 124; judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraphs 82, 170-171.
[14] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraph 227. Although in this case, the interference with PNR agreement was not found to be in violation with Article 47. See further judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 186.
[15] Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 180.
[16] The meaning of the expression 'provided for by law' should be in line with the ECtHR case law, which is frequently cited by the CJEU: an interference shall be based on a provision of law that has certain qualities, also known as the "quality of the law" requirement (judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, EU:C:2016:970; Opinion of Advocate General Saugmandsgaard delivered on 19 July 2016, paragraph 40). The CJEU has referred to a body of ECtHR case law in *La Quadrature du Net*, paragraph 128 in this regard: "*a legal framework should be established enabling a balance to be struck between the various interests and rights to be protected"* (ECtHR, 28 October 1998, *Osman v. United Kingdom*, no. 23452/94 , paragraphs 115 and 116; ECtHR, 4 March 2004, *M.C. v. Bulgaria*, no. 39272/98, paragraph 151. See also: ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 276.
[17] ECtHR, 4 December 2015, *Zakharov v. Russia*, no. 47143/06, paragraphs 228-230; ECtHR, 16 February 2000, *Amann v. Switzerland*, no. 27798/95, paragraph 50; also see EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*, pp. 6-7.
[18] ECtHR, 16 February 2000 *Amann v. Switzerland*, no. 27798/95, , paragraph 56*;* ECtHR, 2 August 1984, *Malone v. the UK*, , no. 8691/79, paragraph 66.
[19] ECtHR, 26 April 1979, *The Sunday Times v. the UK*, no. 6538/74, paragraph 49.
[20] ECtHR, 18 May 2010, *Kennedy v. the United Kingdom*, no. 26839/05; , ECtHR, 29 June 2006, *Weber and Saravia*, no. 54934/00, paragraphs 152, 93-95.
[21] ECtHR, 2 August 1984, *Malone v. the United Kingdom*, no. 8691/79, , paragraph 67; ECtHR, 24 April 1990, *Huvig* v. *France*, no. 11105/84, paragraph 29.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question […]."[22]. The possibility that the surveillance programmes allow access to data (even to data in transit) without sufficiently clear and precise limits was considered a violation of the legality of the governmental access[23]. Such a law needs to have explicit, detailed provisions on surveillance procedures, providing individuals with a sufficient indication regarding the situations in which public authorities may execute surveillance measures and the conditions thereof[24]. As will be further explained below, the legality of the interference is closely related to whether the limitation is necessary and proportionate[25].

1.2.4 OBJECTIVES OF GENERAL INTEREST OR PROTECTION OF RIGHTS AND FREEDOMS OF OTHERS

Governmental access needs to be strictly necessary to comply with **an objective of general interest or to protect the rights and freedoms of others**[26]. An objective of general interest cannot be sought without considering how it must be reconciled with the fundamental rights impacted by the legislation. This is done by appropriately balancing the general interest goal against the rights in question[27]. Therefore, the objective of general interest and the necessity and proportionality of the limitation are closely associated; it is essential to define and clarify the objective of general interest aimed by the limitation in satisfactory detail, as the necessity and proportionality test will be carried out against this context[28].

In that regard, it is worth referring to the case law of the CJEU on data retention, which discusses both the retention of personal data by private operators in order to be accessed by governmental authorities, and the conditions of such access[29]. It is clear from the Court's case law that only the national security objective may justify public authorities having broad access to retained personal data in a general and indiscriminate manner (bulk access)[30]. The national security objective must be linked to a genuine and present or foreseeable serious threat[31].

[22] "*It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted* […]" judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 176.
[23] Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 180; see also judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650.
[24] ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 370.
[25] ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 334.
[26] Article 3 of the Treaty on the European Union, for instance, mentions freedom, security, and justice as general objectives. EDPB (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, p. 11. Article 23 of the GDPR states that data protection can legitimately be limited for security, defence, crime prevention, significant economic and financial interests, public health and social security, provided that the limitation respects the essence of the right to personal data protection and is necessary and proportionate. See also EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*. Relatedly, the CJEU in *Schwarz v. Stadt Bochum* found that processing personal data to prevent illegal entry to the EU pursued an objective of general interest (judgment of the Court (Fourth Chamber) of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670).
[27] Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, paragraph 52; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 130.
[28] EDPS (2017), *Necessity toolkit*, p. 4.
[29] See *Privacy International*, paragraph 73: "*the mere retention of that data by the providers of electronic communications services entails a risk of abuse and unlawful access."*
[30] Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, paragraph 31; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 166.
[31] Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D. v The Commissioner of the Garda Síochána and Others*, C-140/20, paragraph 58; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Targeted access to and retention of traffic and location data are considered by the CJEU to be a serious interference, thus such targeted access must be based on objective evidence which makes it possible to target individuals whose traffic and location data are likely to reveal a direct or indirect link with serious criminal offences[32]. Objective evidence has to be non-discriminatory, e.g., a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending[33]. Moreover, on the basis of objective and non-discriminatory criteria, geographical areas characterised by a high risk of preparation for, or commission of serious criminal offences can be targeted.

An interference with fundamental rights of the EU Charter can also be justified if it is necessary to protect the rights and freedoms of others. The right to personal data protection often ambivalently interplays with other rights, such as freedom of expression and the right to receive and impart information. In such cases, courts must carry out a balancing exercise to settle the tension between the two[34].

1.2.5 NECESSITY AND PROPORTIONALITY

Fundamental rights and freedoms of the EU can be interfered with only if this is strictly necessary[35]. This translates into the requirements of necessity and proportionality[36]. Proportionality requires a balance to be struck between the importance of the public interest pursued and the seriousness of the interference with fundamental rights[37]. Pursuant to the CJEU, proportionality necessitates the presence of minimal safeguards, such as enforceable rights and effective judicial review, in order to guarantee that interferences are "limited to what is strictly necessary", as stated in *Schrems II*[38]. Apart from the cases directly related to international personal data transfers, the CJEU has developed criteria on how to handle the necessity and proportionality assessments in its case law on data retention mentioned above[39]. This case law should be considered relevant also for international personal data transfers that result in governmental access because it explains the limits to such access from the perspective of the EU-Charter[40].

The proportionality assessment extends to the access to and the use of retained data, which should also be limited to what is strictly necessary for the investigation[41]. Authorisation must be asked prior to

[32] Judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2*,C-203/15 and C-698/15, *EU:C:2016:970*, paragraph 111 and judgment of the Court (Grand Chamber) of , 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18, and C-520/18, EU:C:2020:791, paragraph 148.
[33] Judgment of the Court (Grand Chamber) of 5 April 2022, C-140/20, *G.D. v The Commissioner of the Garda Síochána and Others*, EU:C:2022:258, paragraph 78.
[34] For example, the GDPR Article 85 states that the Member States shall reconcile by law the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic, academic, artistic, and literary expression. Freedom of expression and information is ensured by Article 11 of the EU Charter, and limitations on this right must fulfil the criteria in Article 52 (1), provided above. To achieve a balance between two fundamental rights, the limitations of the right to data protection must apply only insofar as strictly necessary (judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan and Satamedia Oy*, C-73/07, ECLI:EU:C:2008:727, paragraphs 56-62).
[35] Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 176 and Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 140-141.
[36] According to the EDPS, the necessity test requires "*a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal*" (EDPS (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*, p. 27, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf. For other views on necessity see: Gerards, J., 'How to improve the necessity test of the European Court of Human Rights', *International Journal of Constitutional Law*, Vol. 11, No 2, April 2013, pp. 466–490, available at: https://doi.org/10.1093/icon/mot004.
[37] Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 130-131.
[38] Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 184.
[39] Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, EU:C:2014:238, paragraph 35.
[40] EDPB (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, p. 7.
[41] Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, paragraph 38.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

access to the data, except in the event of a justified urgency[42]. This review must be carried out either by a court or an independent administrative body whose decision is binding. Moreover, means for individuals to obtain effective judicial and administrative redress should be in place[43]. Data subjects need an effective possibility to access the retained data, obtain rectification, or erase data[44].

The ECtHR has developed minimum safeguards that the national law authorising governmental access should contain in the cases *Weber & Saravia v. Germany*,[45] *Roman Zakharov v. Russia*, and *Big Brother Watch and the Others*[46]. Such laws need to include clear provisions on:

- the nature of offences that may give rise to a limitation;
- the categories of people liable to have their communications intercepted;
- a limit on the duration of interception;
- the procedure to be followed for accessing, examining, using and storing, communicating and destroying the data obtained;
- the precautions to be taken when communicating the data to other parties and the circumstances in which intercepted data may or must be erased or destroyed; and
- the review of the authorisation procedures and arrangements supervising the implementation of the measures along with any notification mechanism and the remedies provided[47]. This last safeguard may come into play when (i) the surveillance is first ordered, (ii) while it is being carried out, or (ii) after it has been terminated[48].

1.2.6 RESPECT THE ESSENCE OF THE RIGHT

In some instances, an interference can be so extensive and invasive it empties an EU fundamental right of its essence[49]. In this regard, the CJEU considered the law allowing public authorities to access, on a general basis, the content of electronic communications as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the EU-Charter[50]. However, in *Digital Rights Ireland*, where the legislation in question did not permit generalised access to content data, the CJEU held that the limitation was not so intrusive as to impact the essence of the right[51]. *Schrems I* noted that legislation that does not provide any possibility to pursue legal remedies, e.g., access to or to rectify personal data, would be incompatible with Article 47 of the EU-Charter, ensuring the fundamental right

[42] Judgment of the CJEU (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, EU:C:2016:970, paragraph 120; judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 137-139; judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, EU:C:2021:152,, paragraphs 40,53-54,58; ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 355.
[43] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 218-227.
[44] *Ibid.* See further judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 190.
[45] ECtHR, 29 June 2006, *Weber and Saravia*, no. 54934/00, also mentioned in judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 175; judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International*, C-623/17, paragraph 65.
[46] ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 54.
[47] ECtHR, 4 December 2015, *Zakharov v. Russia*, no. 47143/06, paragraphs 228-230; ECtHR, 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, no. 58170/13, 62322/14 and 24960/15, paragraph 335.
[48] ECtHR, 25 May 2021, *Big Brother Watch*, paragraph 336.
[49] Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017, EU:C:2017:592, paragraphs 124, 138-141, 150; EDPB (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*, p. 6.
[50] Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14 *EU:C:2015:650*, paragraph 94.
[51] Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, EU:C:2014:238 , paragraph 39.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

to effective judicial protection[52].

The essence of a right is interpreted by legal scholars in two ways. The first approach reads the notion as an absolute limit which is not subject to balancing[53]. Following the first view, where the essence of a fundamental right is violated, the interference is unlawful without a further need for testing its necessity and proportionality[54]. The second view links the essence to proportionality test as explained above[55]. In this view, essence forms one component in the proportionality test.

1.3 STUDY METHODOLOGY

For this study, a literature review via desk research (books, journal articles, databases and other online sources) was conducted as the primary step. The purpose of this review was to map the law in the books, consisting of the relevant legal instruments and relevant case law. In addition, reports of international organisations were compiled in this step. After conducting a legal analysis of the collected sources, the loopholes in the knowledge in this area of law were defined for each country (Mexico, and Türkiye). Thereafter, focus was laid on the law in action. Per country, a customised questionnaire was composed, tackling the higher defined loopholes (see Annex 1). Both country questionnaires were priorly presented to the EDPB, making it possible to distribute the questionnaires to carefully selected experts in each country. To have a broad perspective, the researchers of this study strived to find persons working in different legal fields (academia, non-profit sector, the Bar ...).

We have carried out the following numbers of interviews:

- Mexico: five stakeholders were interviewed, including four lawyers and one representative of academia. The interviews were crucial to understand the Mexican federation system, the different functions of the data protection authorities, and the difference between the legal rules and their application, which has been indicated in the footnotes.
- Türkiye: five stakeholders were interviewed, including three representatives of academia and two practising lawyers from different law firms. The interviews have largely validated the already collected information. The interviews contributed to a better understanding of upcoming legislation, as some of the interviewees had been involved in this process.

Finally, the interviews were carefully analysed and compared with the results of the desk research. Where needed, anomalies were indicated. Based on this, the end report of the in-depth analysis of the countries was drafted including the results of the interviews.

[52] Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, EU:C:2015:650, paragraphs 64 and 95. The same conclusion regarding Article 47 was reached in *Schrems II*, where the Court stated: "*According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter*" (judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559, paragraph 187).
[53] "*From a methodological perspective, the case law of the CJEU reflects the fact that court will first examine whether the measure in question respects the essence of the fundamental rights at stake and will only carry out a proportionality assessment if the answer to that first question is in the affirmative*". Lenaerts, K., 'Limits on Limitations: The Essence of Fundamental Rights in the EU', *German Law Journal*, Vol. 20, pp. 787, 779-793, Cambridge University Press, 2019. See further Brkan, M., 'The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning', *German Law Journal*, Vol. 20, pp. 864-883, Cambridge University Press, 2019.
[54] European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018, p. 44.
[55] Tridimas, T., Gentile, G., 'The essence of Rights: An Unreliable Boundary?', *German Law Journal*, vol. 20, pp. 794–816 and itsp. 804: *"In short, although the concept of essence as a legal threshold must be understood as an autonomous limit, in effect, it is impossible to determine it without engaging in a balancing process which is best carried out through a proportionality analysis."*

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

1.4 STRUCTURE OF THIS REPORT

Section 2 describes an in-depth analysis of the legislation and practice on government access to personal data in Mexico (section 2.1) and Türkiye (section 2.2). The same structure is followed in every country section.

Each country section presents a first subsection aiming to answer the research question concerning the general situation of the countries as regards human rights, and specifically the right to privacy and data protection. It provides an overview concerning the rule of law, respect for human rights and fundamental freedoms in the observed countries. The main constitutional provisions of both countries are analysed, as well as the concrete application of such provisions in the national case law. The subsection also illustrates whether and how the right to privacy exists in both legal systems. Afterwards, the general findings by international organisations on the the countries' human rights situation are also briefly shown.

Subsequently, the country reports include a subsection illustrating the purposes, conditions, and oversight mechanisms of the governmental access to personal data in both countries. This subsection aims to answer the research questions related to the specific legislative requirements for government access to personal data; where specific provisions on foreign individuals' personal data do not always exist in the legal systems, the report also tries to address the research questions around the applicability of the countries' legislation to foreigners.

In each country section, a subsection is dedicated to the data subjects' rights, their conditions for applicability and the redress mechanisms available to enforce them. The subsection's goal is to answer the research questions around individual rights and existing redress mechanisms as regards the right to privacy in the legal systems of both countries.

Section 3 provides conclusions by answering the research questions.

The annexes included to this study entail the exact questionnaires per country (Annex 1), a list of all the used sources (Annex 2) and an overview of the used acronyms and abbreviations (Annex 3).

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

2 IN-DEPTH ANALYSIS OF THIRD COUNTRIES

The following section aims to answer the research questions of the study in relation to both countries. The structure of the subsections is consistent with a division into areas of interests touched upon by the research questions. The answers are integrated in the related subsections. Each section provides an in-depth analysis of the legislation and practice in third countries on their governments' access to personal data. Section 2.1 deals with the situation in Mexico and Section 2.2 with Türkiye. All these sections study the situation in third countries from the perspective of the rule of law and respect for human rights and fundamental freedoms; government access to personal data; and data subject rights. Any potential upcoming changes in the legislation are also discussed. Finally, every country section contains an intermediary conclusion and a grid visually presenting the research results.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

2.1 MEXICO

2.1.1 RULE OF LAW, RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

Mexico is a presidential representative democracy and a constitutional republic. The Mexican Constitution dates from 1917 and there were several amendments throughout the years – the last one being published at the end of 2022.

Privacy has been a fundamental right in the Mexican constitution since its initial text. The right to personal data protection, however, was only included in the Mexican constitution in 2004. The amendment consisted of provisions stating that every person has free access to their personal data and the possibility to rectify their information without justification. In 2017 a specific provision mentioning the right to data protection was added to the constitution.

The constitutional text already sets a list of minimum individual rights that should apply to all processing of personal data. These are the ARCO rights, namely access, rectification, cancellation, and objection to processing[56]. Another individual right is the possibility to oppose the disclosure of personal data. The ARCO and other data protection rights are constitutional, thus applied to every person, regardless of their nationality. Any restriction to these individual rights must be justified by reasons of national security, law and order, public security, public health, or the protection of fundamental rights of third parties. Such limitations are implemented by a specific law – the National Security Law (NSL)[57]. Reaffirming the general aspect of the right to data protection, the Mexican Supreme Court ruled that the principles of data protection apply when data are shared with a public authority[58].

The constitution requires that Mexico establishes an autonomous, specialised, impartial, and independent authority to be responsible for transparency and access to public information and data protection. Such an authority is then responsible to oversee the data processing controlled by private and public parties (Article 5, VIII Constitution). Based on this provision, the National Institute for Transparency, Access to Information and Data Protection (INAI)[59] was created. The body has published many guidelines and recommendations, such as the Guidelines for the Processing of Biometric Data[60]. Besides its normative work involving publishing guidelines and other documents, the INAI issues yearly reports on the activities it carries out[61].

The role of the guidelines issued by the INAI differs depending on to whom they are addressed. Guidelines for the public sector should be observed, considering the INAI's role as a second instance of oversight of data protection activities. But documents that address private parties are non-binding and cannot be used in court, as ruled by the Supreme Court. The Supreme Court clarified that "*[…] it is possible to determine that the INAI is only entitled to issue internal administrative regulations or ordinances with purposes to regulated aspects related to its functioning and operation, is strict*

[56] Article 16, §1, Mexican Constitution establishes: "*All people have the right to enjoy protection of his/her personal data, and to access, correct and cancel such data. All people have the right to oppose the disclosure of his/her data, according to the law. The law shall establish exceptions to the criteria that rule the handling of data, due to national security reasons, law and order, public security, public health, or protection of third party's rights.*"
[57] *Ley de Seguridad Nacional, de 31 de enero de 2005*.
[58] Case n. 2005522, Thesis P. II/2014, 21 January 2014, summary of the decision: "*Judicial persons. They have the right to the protection of the data that may be equal to personal data, even if such information has been delivered to a public authority*."
[59] Instituto Nacional de Transparencia, *Acceso a la Información y Protección de Datos Personales*.
[60] Available at: https://inicio.inai.org mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf.
[61] INAI, *Informe de Labores* 2022, available at: https://micrositios.inai.org.mx/informesinai/.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

congruence with the constitutional text, especially since it does not have the power to legislate on the substantive matter of protection of personal data held by private companies"[62].

Internationally, Mexico has a strong presence in Conventions regarding human rights. The country has ratified the Universal Declaration of Human Rights, the International Convention on Civil and Political Rights, the International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families and Convention 108 and its additional protocol. More recently, the country has signed the OECD's "Declaration on Government Access to Personal Data Held by Private Sector Entities"[63]. Regionally, Mexico has ratified the American Convention on Human Rights, and is part of the Inter-American Court of Human Rights.

The country's legal system is based on civil law and codified laws. Data protection is regulated by two main laws – one focused on the private sector and the other one on the public. For companies (the private sector), the Law on the Protection of Personal Data in the Possession of Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares* - LFPDSSPP) became applicable in 2010. The LFPDSSPP sets out a series of principles and procedures that should be observed by controllers of personal data; it already establishes that the principles and rights foreseen in the law can be limited for purposes of national security, public order, security, health, and third parties' rights[64].

After seven years, to avoid a legal gap in cases where the LFPDSSPP does not apply, the Law on the Protection of Personal Data in the Possession of Public Parties (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* - LGPDSSO) was adopted in 2017. The law applies to any federal, state, or municipal public body, including every authority of the executive, legislative and judicial powers, political bodies, and public funds, including law enforcement authorities. Thus, differently from what is regulated by the LFPDSSPP, the LGPDSSO applies directly to the public sector. Following the constitutional provisions, the law reaffirms that the right to data protection may only be limited for purposes of national security[65], public order, security, health, and to protect third parties' rights[66].

The LGDPSSO also addresses the right to access public data, mentioning the National System of Transparency, Access of Information and Data Protection[67]. This shows the importance of the General Law of Transparency and Access to Public Information (*Ley General de Transparencia y Acceso a la Información Pública* - LGTAIP). The LGTAIP establishes common rules to public authorities when implementing the principle of transparency. The law also addresses some proportionality issues related to access to public data and the fundamental right to protection of personal data.

According to the interviewed national experts, the National Code of Criminal Procedures is the most relevant law on regulating surveillance activities carried out by law enforcement authorities[68]. Additionally, Mexico has a National Security Law (NSL), which, as mentioned above, sets rules on data processing for national security purposes. Thus, there is no legal gap on data processing for these purposes, since the NSL establishes the rules for these activities.

Mexico is a federation; thus, various levels of legal and government systems co-exist[69]. This can lead to difficulties when implementing legal reforms by the Mexican federal government, especially in the field of human rights. With the involvement of international bodies and civil society, new regulations bring

[62] Amparo Directo en Revisón 6489/2018.
[63] The complete text of the document is available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.
[64] Article 4 of the LGPDSSPP.
[65] Usually, intelligence activities fall under this exception.
[66] Article 6 of the LGPDSSO.
[67] Sistema Nacional de Transparencia, *Acceso a la Información y Protección de Datos Personales*.
[68] Interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.
[69] Mexico has 33 jurisdictions, composed of 31 states, Mexico City and a federal jurisdiction.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

obligations to all levels of government, including rules of transparency in public authorities and data protection. The new developments bring more uniformity to the Mexican legal system[70].

In terms of legislation, the fact that Mexico is a federation is noticeable in the different types and levels of legislation[71]. In states and municipalities, local laws can be developed. National Congress can publish federal, general or national laws. Federal laws are adopted in accordance with the competences attributed to the National Congress. General laws outline the regulation of a topic determined by the Constitution, harmonising the system while dividing competences. Federal entities must observe the provisions set by the general law, even when legislating on the details of the topic. Other levels of laws cannot modify what is established by the general law. National laws are always linked to the constitutional attribution of the distribution of competences[72].

The characteristics of the federal system are also visible in the regulation and oversight of data protection. Regarding processing activities carried out by public authorities, the general law (LGPDSSO)[73] establishes general guidelines that shall be observed by local levels, while dividing competences[74]. Nonetheless, each federal entity incorporates the general rule locally, determining how the provisions and competences set by the LGPDSSO will be applied locally[75]. Based on the federal constitution[76], each local constitution or law also establishes an authority responsible for overseeing the data processing and transparency activities carried out by public entities in that region, while the local authorities' activities are assessed by the INAI. This system is reaffirmed by the LGPDSSO.

Personal data processed by private entities is a federal competence[77], this means that there are no local laws on the matter[78]. Therefore, the INAI is the competent authority to oversee the data processing activities by private parties, not dividing this competence with local bodies. However, a ruling from the Supreme Court stated that the constitutional provision that foresees this competence (Article 73, XXIX-O) does not include the power to issue general and abstract rules on this topic. The National Congress is the body responsible for such rules[79].

Considering the impossibility of analysing in detail all the different regional and local legislations, this study focuses on the general laws and on the LGPDSSP. Regarding other topics that are relevant to the scope of the study, the different types of laws are taken into account. Such an approach addresses the

[70] García, A., *Transparency in Mexico: An Overview of Access to Information Regulations and their Effectiveness at the Federal and State Level*, 2016, Report, Wilson Center Mexico Institute.
[71] The Supreme Court ruled that there are five different legal orders in Mexico: "*the federal, the local or state, the municipal, the Federal District, and the Constitutional*", Suprema Corte de Justicia, Controversia Constitucional, P.J., 136/2005.
[72] Estrada, J. M. M., 'Configuración normativa de las leyes en el marco competencial de los órdenes jurídicos', *Congreso Redipal Virtual VIII*, Marzo 2015, available at: https://www.diputados.gob mx/sedia/sia/redipal/CRV-VIII-14-%2015.pdf; Tópez, S.T.,'Sustitución de la Ley Federal de Archivos de México: el alcance de una ley general', *Revista Española de la Transparencia*, no 12, Jan-Jun 2021, Estado de México, Periódico Oficial Gaceta del Gobierno y Legistel, Leyes Nacionales, Generales y Federales, pp. 167-187, available at: https://legislacion.edomex.gob.mx/leyes_federales.
[73] Article 73 Mexican Constitution: "*The Congress shall have the power to: XXIX-S. To issue general regulating laws that establish the principles and basis in regard to government transparency, access to information and protection of personal data held by authorities, entities or government agencies at all levels of government."*
[74] One of the objectives of the LGPDSSO is to distribute competences between the federal and local oversight authorities in matter of data protection processed by public entities (Article 2, I, LGPDSSO).
[75] Article 9, §1, Mexican Constitution.
[76] Article 116, VIII, Mexican Constitution: "*The local constitutionas shall establish specialised, impartial, collegiate and autonomous entities responsible for guarantee the right of access to information and the protection of personal data held by public parties, following the principles and fundamental established in the Article 6 of this Constitutional and the general basis, principles and procedures to exercise these rights stated by the general laws issued by the Mexican Congress*".
[77] Lopes, T. M. G., 'Las recientes reformas em materia de protección de datos personales em México', *Anuario Jurídico y Económico Escurialense*, XLIV, 2011, ISSN: 1133-3677, Mexico, pp. 317-334.. Lineamientos Generales de Protección de Datos Personales para el Sector Público, available at: https://www.gob.mx/cms/uploads/attachment/file/304930/lineamientos_generales_para_la_protecci_n_de_datos_personales_para_el_sector_p_blico.pdf.
[78] Article 73 Mexican Constitution: "*The Congress shall have the power to: XXIX-O. Regulate the use and protect personal data handled by private entitites*".
[79] Amparo Directo en Revisón 6489/2018.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

main objective of the work, especially since the general laws shall be transposed in the regional regulations. Therefore, this approach allows the evaluation of the main provisions in Mexico, while also giving an overview of the topics that are further regulated locally. The following table summarises the laws evaluated in this work and the different legal scopes:

Law	Year of publication	Scope	Local and federal legislations?
Ley de Seguridad Nacional	2005	General	No
Ley Federal de Protección de Datos Personales en Posesión de los Particulares	2010	Federal	No
Código Nacional de Procedimientos Penales	2014	Federal and local judicial bodies	Yes[80]
Ley General de Transparencia y Acceso a la Información Pública	2015	General	Yes
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	2017	General	Yes

2.1.1.1 TRANSPARENCY RULES AND DATA ACCESS

Since 2002, state laws have been in force in different Mexican regions on transparency and data access. In 2007, Article 6 of the Constitution was amended to regulate the principle of transparency and the right to access information[81]. The General Law for Transparency and Access to Public Data (LGTAIP)[82] was created in 2015 to implement the constitutional provisions about the principle of transparency and access to information in the public sector. Following the Mexican legal system, this general law establishes minimum bases for the topic of transparency and access to public data, while dividing competences with states and the Federal District. Thus, there are regional laws operationalising the general law.

The final text of the LGTPAI was the result of the work of a multisector group established by Congress, which provided for stricter provisions on judicial and societal control over the government's activities. The fact that corruption is put as one of the scenarios where information cannot be withheld, considering all the previous claims of human rights' violations, exemplifies this scenario. Another relevant provision is the obligation of publicising the rulings of the Mexican Courts, especially the binding ones. The law also increased the competences of oversight bodies. Each state, Mexico City and the federal government had to create an independent and specialised oversight authority to guarantee compliance with the provisions on transparency. The federal authority is the INAI.

This scenario led to the creation of the National Transparency System[83]. Its role is to coordinate and evaluate the actions related to transparency, access to information, and personal data protection, and to establish and implement criteria and guidelines[84]. For this, the System is also responsible for organising the use of the National Transparency Platform (*Plataforma Nacional de Transparencia*), while promoting the right to access to public information and personal data for the purposes of the LGTAIP.

[80] The Code of National Procedures harmonises the criminal procedures throughout the whole country, for local or federal judicial bodies, thus, federal or local crimes. However, local criminal codes still exist. Mexico, Senado de la República, Código Nacional de Procedimientos Penales, 2014, available at: senado.gob mx/comisiones/justicia/docs/CNPP.pdf.

[81] These provisions follow the principle of maximum disclosure, defined by Article 8, VI, of the LGTAIP as "*every information in the control of public authorities must be public, complete, timely and accessible, subjected to an exception regime that must be defined and legitimate and strictly necessary in a democratic society*".

[82] *Ley General de Transparencia y Acceso a la Información Pública* (LGTAIP).

[83] Sistema Nacional de Transparencia, *Accesso a la Información Pública y Protección de Datos Personales*.

[84] Article 28, LGTAIP.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

The following bodies are part of the National Transparency System[85]:

- the INAI;
- the local oversight bodies[86];
- the General Auditor's Office *(la Auditoría Superior de la Federación);*
- the National General Archive (*el Arichivo General de la Nación*); and
- the National Institute for Statistics and Geography (*el Instituto Nacional de Estadística y Geografía*).

Even though the main oversight focus is related to the management of public assets, the use of personal data is also a topic of discussion in the LGTPAI. The need for balancing the rights of access to information and data protection is acknowledged in the law[87]. Thus, while developing their activities, public authorities must consider the protection of personal information in parallel to transparency rules. Non-personal data is to be accessible, except for a determined period and for reasons of public interest or national security[88]. With these considerations, public authorities may decide on data access requests. Their decision can be subject to a revision claim *(recurso de revisión*).

In fact, any individual can make a revision claim in front of the local competent authority. The LGTAIP established that the following topics can be discussed in such claims:

- classification of information (confidential, reserved or public);
- declaration of inexistence of the information;
- declaration of incompetence by the public authority;
- providing incomplete information;
- delivering different information to what was requested;
- lack of response of an access request in time;
- delivering of information in a different format to the requested;
- the costs or time frame for the access of information;
- lacking a procedure for a request;
- denying direct consultation to the information;
- insufficient justification in the response of the public authority; or
- the rules published by a public authority on a specific procedure, e.g. for the right of access.

Other topics may be discussed in revision claims as long as they relate to the right of access to public information. To do this, the individuals should justify their claims on the basis of the LGTAIP or other relevant legislation, including national and international rulings or opinions on transparency[89].

The revision claims will then be analysed by the competent authority. Actions of federal bodies should be presented to the INAI. In other instances, activities of state or municipal bodies will be overseen by the local authorities. The system has the local oversight bodies as the first instance, since all the decisions of these bodies are overseen by the INAI[90]. Judicial bodies can overturn and supervise the decisions

[85] Article 30 LGTAIP; Article 31 of LGTAIP establishes all the functions of the National System.
[86] Each federal entity has to establish an autonomous authority for transparency and data protection. The INAI acts for the federal level. However, there are 31 state authorities and one authority for the Federal District.
[87] Article 23 of the LGTAIP "*The following entities are obliged to publish and allow the access to information and to protect the personal data under their control: any authority, entity, body or organ of the Executive, Legislative and Judicial Power, autonomous bodies, political parties, fiduciaries and public funds, as any other person – private or legal – or union that receives and uses public assets or perform authority activities in federal, state or municipal scope*."
[88] Article 4 of the LGTAIP. However, information related to severe violations of human rights or to crimes against humanity can never be classified as reserved.
[89] Article 7 paragraph 2 LGTAIP "*For interpretation purposes, criteria, rulings and opinions from national or international organisms, in transparency topics, can be taken into account*."
[90] The System is composed of the INAI, local oversight bodies, the Federal Audit Office, the General Archive and the National Institute of Statistics and Geography.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

taken by the INAI or the other local oversight bodies, as explained further below. A specialised body to oversee public policies on topics of transparency and data access also exists[91].

Article 68 LGTAIP establishes minimum rules about data protection in public authorities, which include the need to respond to requests related to subjects' rights and guaranteeing the application of the principles of necessity and quality[92]. This provision also sets transparency rules, stating that public authorities need to provide a public document with the purposes of data processing. However, this transparency obligation does not apply to cases where the processing is based on the legal basis of performance of legal duties[93].

Only in case of explicit consent can the public authorities share[94] the personal data under their control[95]. The consent is not needed when the information is public, when there is a legal ground for this processing, when there is a judicial order, or for reasons of national security, general health or to protect rights of a third person. The data subject's consent is also not needed when the sharing happens between public authorities or international law bodies, if this is foreseen in a treaty and if the information is used for the activities developed by those authorities. The same rules apply to requirements of access to confidential information[96].

Considering that the LGTAIP is from 2015, nowadays the data protection rules set by this law only apply if compatible with the specific laws on data protection in the public sector set by the more recent rules in the LGPDSSO, discussed in the following section. In other words, while the LGTAIP remains to be the specific law for transparency rules, the LGPDSSO – from 2017 – takes on the leading role as the specific norm for data protection in the public sector.

2.1.1.2 DATA PROTECTION IN THE PUBLIC SECTOR

The LGPDSSO is the most relevant law on data protection in the public sector, laying down its general aspects for data protection. In addition to the LGPDSSO, the INAI has published binding general guidelines on the matter[97]. The LGPDSSO establishes competences for each state entity (federal, state, and district) to apply and oversee the general provisions.
Public authorities must always justify the processing of personal data controlled by them. This includes informing individuals about its purposes, which must be legal, explicit, and legitimate. All these activities must be connected to the public powers of the controlling body[98]. Consequently, public authorities must provide a privacy notice with minimum information about the processing[99]. In case of

[91] García, 2016.
[92] Article 68, II "*[controllers are obliged] to process personal data only where such data is adequate, relevant and not excessive in relation to the purposes for which they were collected, or such processing is carried out in the exercise of the powers conferred by law*". Article 68, V "*[controllers are obliged] to replace, rectify or complete, ex officio, any personal data which is inaccurate, incomplete, wholly or in part, at the time they become aware of this situation*".
[93] Article 68, III of the LGTAIP "*The obliged subjects are responsible for the personal data under their control and must: III – make it available for individuals, from the moment of the data collection, the document that establishes the purposes of the processing, according to the legal rules that apply, except in cases in which the processing is based on the performance of legal duties.*"
[94] Even though the LGTAIP mentions the selling of data, it seems that this possibility was overturned by the LGPDSSO, since this law is more specific on data protection and more recent. Article 68 paragraph 1 LGTAIP establishes that "*public authorities, cannot share or commercialize personal data that are part of the information systems developed in the exercise of their public functions, unless they receive express consent, written or by a similar authentication system, of the individuals that the information relates to. This applies without prejudicing what is established by Article 120 of this law*."
[95] Article 68 of the LGTAIP.
[96] Article 120 of the LGTAIP.
[97] *Lineamientos Generales de Protección de Datos Personales para el Sector Público*, available at: https://www.gob.mx/cms/uploads/attachment/file/304930/lineamientos__generales_para_la_protecci_n_de_datos_personales_para_el_sector_p_blico.pdf.
[98] Article 18 of the LGPDSSO.
[99] The minimum content of privacy notices is established by Article 27 of the LGPDSSO.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

the impossibility of making the notice available to the individual, the authority can apply a compensatory measure in the form of mass communication to disseminate the information[100].

Free, specific and informed consent[101] is the general rule for the processing of personal data in the public sector[102]. Due to the imbalance of powers in the relationship between individuals and the government, having informed consent as a general rule for processing can be problematic. Therefore, the legal system provides for additional legal grounds for data processing[103] so that consent is not always mandatory. These are:

- processing is established by law, that does not contradict the LGPDSSO;
- the data processing is for a compatible purpose to the one that was set for the initial processing;
- there is a judicial order;
- processing is necessary for the recognition or defence of the subject's rights before a competent authority;
- processing is necessary for exercising a right or complying with obligations derived from a relation between data subject and the controller;
- processing is required in an emergency situation that can result in harm to individuals or their assets;
- processing is necessary for health care or sanitary reasons;
- processing relates to public information[104];
- processing of anonymised data; or
- when the personal data concerns a missing person, according to a specific law.

The processing of sensitive data by public authorities is prohibited unless the explicit consent of the data subject is collected or unless one of the general consent exceptions mentioned above applies[105]. Consent is also needed for a legitimate processing of personal data for a secondary purpose, not mentioned in the privacy notice. The purpose not published must be related to the legal competences of that public authority[106]. The exceptions for consent do not apply for secondary purposes.
Since the law establishes various exceptions for the content rule, the INAI suggests in their guidelines that public authorities clearly identify the purposes of the data processing, also stating which processing operations are based on consent and which are not[107].

For processing of data of minors, the principle of the best interest of the minor shall prevail and the public body must also comply with specific regulations on the topic[108].

Consent is also a standard legal basis to justify national or international data transfers. However, there are various exceptions to said rule. The exceptions that justify data processing without consent outlined above also apply for data transfers. In addition, there are other exceptions that also remove the need for

[100] Article 26 of the LGPDSSO.
[101] In the general cases, consent can be both express or tacit, as mentioned by Article 21 of the LGPDSSO.
[102] Article 20 of the LGPDSSO.
[103] Established by Article 22 of the LGPDSSO.
[104] The LGPDSSO establishes that the following categories are considered as sources of public information: internet websites and other electronic communications media that facilitate access to data to the public and have unrestricted access; phone books, official diaries, and publications; social communication media; and public registries.
[105] Article 7 of the LGPDSSO establishes "*As a general rule, sensitive personal data may not be processed, unless there is the express consent of the subject or, failing that, in the cases established in Article 22 of this Law*".
[106] Article 18, Paragraph 1, of the LGPDSSO establishes: "*the controller may process personal data for purposes other than those established in the privacy notice, as long as it has powers conferred by law and collects the subject's consent, unless it is a person reported missing, under the terms provided for in this Law and other provisions that are applicable in the matter*".
[107] INAI, *El ABC del aviso de privacidad*, Sector Público, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_ABC-AP-SPublico.pdf.
[108] Article 7, Paragraph 1, of the LGPDSSO.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

consent for data transfers. Thus, in the following additional cases, a data transfer is also justified without the need of the subject's consent[109]:

- when the transfer is foreseen in laws and international agreements or treaties;
- when the transfer is legally foreseen for criminal investigations or prosecution, as well as for law enforcement;
- when the transfer is governed with contractual or pre-contractual provisions of an instrument that the processing entity is part of;
- when the transfer is necessary for the maintenance of a judicial relationship between the controller and the subject, including for the exercise of rights or fulfilment of obligations;
- when the transfer is necessary for national security reasons.

Even though the LGPDSSO explicitly states that international or national data transfers can occur without the subject's consent in the exceptions foreseen in Articles 22, 66, and 70, outlined above, the application of these exceptions is not completely clear. For example, Article 22 establishes that consent is not necessary when the purpose of the data processing is the recognition or defence of the subject's rights before a competent authority. However, Article 70 adds an additional requirement for this scenario: the authority must request the data. Thus, it is uncertain if all the conditions for exceptions foreseen in Article 70 must be observed for data transfers.

Any data transfer involving a public authority must be formalised through contractual clauses, collaboration agreements, or any equivalent legal instrument. This obligation does not apply to national transfers that occur in order to comply with a legal provision or to exercise legal competences provided by the law[110]. The need for a legal instrument is considered fulfilled if a treaty of law already foresees the international transfer[111].

Based on the outlined provisions, international data transfers to third countries can therefore happen without the prior consent of the data subject if the above exceptions apply, meaning whenever this activity is foreseen in a Mexican law or a treaty. The same applies to international transfers carried out after a request of a foreign authority, if the purposes of the transfer are equivalent to the ones that justified the initial processing[112]. This means that whenever the third country's purposes are compatible with the reasons why the processing of personal data started, the data transfer can happen without the subject's consent and without the need of a specific treaty or law. In any case of a data transfer to third countries, the recipient is obliged to protect the data according to Mexican law[113], which needs to be verified by the controller[114].
The INAI can publish a technical opinion on an international transfer, which can be positive or negative. It will issue such an opinion after the request of a representative. If the INAI does not publish the technical opinion within the time frame set by law, it should be understood that the authority is not favourable to the transfer[115].

Finally, the LGPDSSO mentions the obligation of applying security measures to guarantee the protection of personal data by public authorities[116]. Adopted security measures need to be documented

[109] Articles 22, 66 and 70 of the LGPDSSO.
[110] Article 66 of the LGPDSSO.
[111] Article 66, II of the LGPDSSO.
[112] Article 66, II of the LGPDSSO.
[113] Article 68 of the LGPDSSO.
[114] INAI, *Recomendaciones para los sujetos obligados en las comunicaciones de datos personales*, May 2022, available at: https://home.inai.org mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones-SO_Comun_DP.pdf.
[115] INAI, *Recomendaciones para los sujetos obligados en las comunicaciones de datos personales*, May 2022, available at: https://home.inai.org mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones-SO_Comun_DP.pdf.
[116] Article 31, LGPDSSO "*Regardless of the type of system in which the personal data are held or the type of processing carried out, the controller must establish and maintain administrative, physical and technical security measures for the protection of personal data, in order to protect them against damage, loss, alteration, destruction or unauthorised use, access or processing, as well as to guaranteeing their confidentiality, integrity and availability*".

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

in a specific security document[117], which needs to be updated whenever there are substantial changes in the data processing, affecting the risk level in terms of data security[118]. The LGDPSSO does not set any further details on these security aspects, such as minimum standards.

2.1.1.3 FURTHER PROCESSING OF PERSONAL DATA BY PUBLIC AUTHORITIES

Mexico's Constitution establishes that public authorities can only temporarily retain information for the purposes of public interest or national security, according to the relevant legal provisions obliging those authorities to record their activities[119]. This provision leaves room for a bigger societal and international scrutiny of the government's activities, since time becomes another factor of control. To implement this, Mexico has established different rules about transparency and data access (LGTAIP), which were mentioned earlier in this report, in parallel with a specific legislation about national security.

The LGTAIP establishes that every authority is responsible for classifying the level of access to the information they use. As mentioned, as a rule, personal data is considered as confidential data. Bank, fiduciary, industrial, commercial, fiscal, stock exchange and postal secrecy information are also considered confidential. As a rule, public authorities must therefore receive the consent of the data subject to allow the access to confidential information. However, the consent is not needed if the information: (i) is available in public databases; (ii) has public status set by law; (iii) is part of a judicial order for access; (iv) is needed for national security, health care or for the protection of third parties' rights; (v) is shared between public authorities or international bodies, following treaties, or (vi) when the information is needed for their activities.

In other cases, information can be classified as 'reserved', making it thereby more difficult to access or disclose. Article 113 of the LGTAIP sets that an authority can label information as reserved if: (i) it compromises the national or public security, or national defence, as long as it has a genuine purpose; (ii) can affect international relations; (iii) was delivered to Mexico as reserved or confidential information, as long as it does not affect human rights; (iv) brings risks to the economic and monetary system of the country; (v) brings risks to a person's life, security or health; (vi) obstructs the enforcement of the law or the payment of taxes; (vii) obstructs the prevention or persecution of crimes; (viii) contains information about the deliberation process of public servants, while there is no final decision; (ix) obstructs the procedures of liability of public servants, while there is no final administrative resolution; (x) affects the due process of law; (xi) affects a judicial or administrative procedure; (xii) is part of a criminal investigation under the Prosecutor's office; (xiii) is foreseen in a law or international treaty.

A ruling by the Mexican Supreme Court of Justice found that public authorities can principally disclose confidential information, for example in response to an access request, including personal data after having conducted a risk assessment. To prevent disclosure of information, public authorities must therefore demonstrate significant risks of harm to the public interest or national security to justify the classification of information as reserved or confidential[120].

[117] Article 35, LGPDSSO, "*In particular, the controller shall draw up a security document containing at least the following: I- the inventory of personal data and processing systems; II – the functions and obligations of persons processing personal data; III – risk analysis; IV – gap analysis; V – the work plan; VI – the mechanisms for monitoring and review of security measures; and VII – the general training programme*".

[118] Article 36, LGPDSSO: "*The controller must update the security document whenever the following happens: I – there are substantial changes to the data processing that result in a change in the level of risk; II – as a result of a process of continuous improvement, derived from the monitoring and review of the management system; III – as a result of an improvement process to mitigate the impact of a breach of security that has occurred; and Iv – implementation of corrective and preventive actions in response to a security breach".*

[119] Article 6, A, I of the Constitution.

[120] Case n. 2018460, Thesis I.10o.A.70 A (10a), Supreme Court of Justice. November 2018.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

As a rule, it is therefore prohibited to disclose information that reveals personal data, including providing access to such data[121]. Nevertheless, the LGTAIP also establishes that each entity is autonomously responsible for defining the classification of and the access to information. This also applies to information gathered for national security purposes[122].

2.1.1.4 GENERAL FINDINGS OF INTERNATIONAL ORGANISATIONS

In the last 15 years, Article 19 has documented and criticised the restrictions against freedom of expression and lack of government transparency. The organisation has worked side-by-side the government in creating and implementing transparency rules to act against corruption scandals. However, the regional office of the institution has received several threats recently[123]. In that regard, national experts have also highlighted the high number of corruption cases involving Mexican authorities[124] and the government pursuit to diminish the power provided to the INAI. For instance, there were news articles regarding the governmental attempts to discontinue the INAI[125].

Moreover, the Mexican government is increasingly relying on new surveillance technologies. Especially in touristic areas, these instruments are being adopted to allegedly bring incentives to tourism, advertising more security. These technologies are usually bought by regional governments, which may bring difficulties for the access and exploration of federal oversight mechanisms. And, even at the federal level, there are few regulations on how surveillance technologies can be acquired by Mexican public authorities[126]. Such lack of regulation may lead to governmental access to personal data outside the scope of the LGPDSSO.

The national experts have highlighted that the lack of Mexican regulation on cyber surveillance allows the general use of these technologies, which can be seen in the complaints filed by reporters and human rights' advocates indicating that they have been tracked with said instruments. Even though there are different laws that establish systems of protection, the national experts have elucidated that it is not clear who is responsible for the oversight of these activities[127]. Thus, the supervisory judge foreseen in the Criminal Procedures Code is the only responsible authority for setting boundaries, instead of establishing them explicitly in regulations.

2.1.2 GOVERNMENT ACCESS TO PERSONAL DATA

2.1.2.1 CRIMINAL PROCEDURE

Personal data can be accessed for the purposes of criminal procedures in Mexico when the personal data is necessary to initiate a criminal investigation or to support a criminal accusation. The personal data must be obtained in accordance with the applicable laws and regulations. Additionally, the individual whose data is being accessed must be informed of the purpose of the access.

[121] Article 64 of the NSL.
[122] Article 50 of the NSL.
[123] Article 19, 2022.
[124] The BTI Index was mentioned by the national experts as a way to illustrate the corruption level in Mexico, available at: https://bti-project.org/en/reports/country-report/MEX.
[125] Human Rights Watch (2019), *México: La transparencia y la privacidad, amenazadas*, available at: https://www.hrw.org/es/news/2021/01/28/mexico-la-transparencia-y-la-privacidad-amenazadas.
[126] CNDH, 2022.
[127] Interview conducted on 8 March 2023 with a representative from a public research institution. Similar remarks were made in an interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Different bodies have separate roles on the access to personal data by public bodies for the prevention and investigation of criminal actions. The Criminal Procedure Code (CNPP)[128] is the norm that defines the unified rules to all the Mexican jurisdictions[129] and establishes:

- the role of the police: working under the instructions of the public prosecutors' agencies, the police is responsible for the investigation of crimes;
- the role of the public prosecutors' agencies: conducting the investigation, coordinating the police forces and the experts, deciding about moving forward with a prosecution and ordering relevant actions to guarantee enough evidence for a conviction or acquittal.

As a rule, following the LGPDSSO, the data subject should be notified about any processing of their personal data, including for law enforcement activities. However, to enable some investigation activities, the CNPP establishes cases in which the subject will not be notified in advance about the access to their personal data. There are therefore two investigatory measures, that can take place without previous notification of the subject: (i) interception of private communications and (ii) access to geolocation data. Law enforcement agencies can thus access private communication or geolocation data for investigation purposes, as further explained below. While the data subject is not notified in these scenarios, a Court will be involved to guarantee the proportionality of the measures.

Prosecution authorities – or their delegates – can request a court[130] to authorise the intervention on private communications[131], justifying the object and need of said activity. A judicial order is also required in cases of extraction of information[132] and to extend the intervention to another person[133]. The intervention can last up to six months. This period cannot be prolonged, except when the prosecution officer can prove that there are new justifying elements[134]. An intervention cannot happen when the request is related to electoral, fiscal, mercantile, civil, labour, or administrative topics. Another limit is the communication between the arrested and his/her lawyer[135].

The public servants authorised to execute the activity are responsible for complying with the terms of the judicial order[136], and all persons involved in the measure must maintain the secrecy[137]. The police or the experts involved in the intervention activity must register the information guaranteeing its quality, so that it can be used as evidence in the procedure[138]. Not following the rules of the surveillance procedure leads to the inadmissibility of the evidence and can lead to administrative or criminal liability of the responsible officer[139]. The appropriate judicial body will order the destruction of unnecessary or unlawful data. The exclusion of information will also happen when the procedure is dismissed or definitively archived, or with the acquittal of the investigated person[140].

[128] *Código Nacional de Procedimientos Penales, de 5 de marzo de 2014*.
[129] The CNPP was the first unified Code about criminal procedures. Before the norm was put into force, there were 33 different codes about this matter in Mexico – one for each jurisdiction.
[130] Suitable federal judge expert in control (*Juez federal de control competente*).
[131] Private communications are defined as "*the whole system of communication or the applications products of technological evolution, that allow the exchange of data, information, audio, video, messages, and also the electronic file that record, retain the content of the conversations or that register the data that identify the communication, which can be presented in real time*" (Article 291 of the CNPP).
[132] Extraction of information is defined as "*the collection of private communications, data that allows the identification of the communication. Also, the information, documents, text files, audios, images or videos retained in any device, accessory, electronic instrument, informatic equipment, retaining devices and everything that may contain information, including the ones storage in platforms or in remote data centres*." (Article 291 of the CNPP).
[133] Article 296 of the CNPP.
[134] Article 292 of the CNPP.
[135] Article 294 of the CNPP.
[136] Article 291 of the CNPP.
[137] Article 302 of the CNPP.
[138] Articles 297 and 298 of the CNPP.
[139] Article 299 of the CNPP.
[140] Article 300 of the CNPP. When there is a temporary archive of the procedure, the information can be retained until the offence is prescribed.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

A similar procedure must be followed for accessing geolocation data or sharing the retained data by the telecommunication companies[141]. The prosecutors' agencies will request the suitable court to authorise the sharing of said communication, explaining the reasons and purposes of the measure[142]. The Code does not mention a specific time limitation of this sharing.

In cases of danger of maintaining the physical integrity or the life of a person, or when the victim of the crime is in danger, or in cases related to abduction of a person, the prosecutor officer will directly command the sharing of the geolocation data or the retained data. In these circumstances, the prosecutor agent or the capable person works under personal liability. The authority must notify the responsible court about the measure within 48 hours, so that the measure can be confirmed – partially or totally. The court can also not ratify the measure, making the information collected inutile for the criminal procedure.

Similarly, the prosecutor or the delegated agent can request the telecommunication companies to retain data contained in networks, systems, or computer equipment. This measure starts immediately after the request or the judicial order[143] and can last up to 90 days[144].

Competent courts provide oversight for the activities described above.

For access to personal data in communications, the law is not clear on whether data subjects are at any point notified about these measures. Whenever data subjects become a part of the criminal procedure, they can get access to information about surveillance matters. However, if they never formally become a part of the procedure (e.g. if they are never charged), they may never be notified about the access to their communications. This is because there is no obligation of prior notification, as explained above, and it is not clear in the CNPP whether there needs to be a mandatory notification after the execution of the activity[145]. In the interviews with national experts, one expert clarified that "*recently, there was a big reform on the telecommunication field. Legal obligations were set on telecommunication companies to record and have available all the data related to the services they provide. A platform was created to process all the requests of access to these databases. Nowadays, telecommunication companies have one main obligation that is to maintain the data and to use this platform to be in contact with the authorities. The new systems also brought obligations to the public authorities to always use this platform for requesting information for telecommunication companies. Even though there were relevant changes, the transparency obligations are still there. What has changed is the way used to comply with the obligations. Currently, telecommunication companies must use the mentioned platform for access in the telecommunications field*" [146]. The national experts also explained that, "*there is no transparency report that has been able to provide information about how often interceptions occur*"[147].

[141] Telecommunication companies shall be understood as any company authorised or operator of telecommunication, and access providers, established by Article 303 of the CNPP.
[142] Article 303 of the CNPP.
[143] This measure follows the same procedure as what is set by the access to geolocation data and its exception in case of imminent danger.
[144] Article 303 of the CNPP.
[145] This was pointed out to the authors in an interview on 2 March 2023, with representatives from a leading Mexican law firm. The experts noted: "*There are no rules about the need to notify the subject. For investigation purposes, the individuals are not notified that they are being targeted with a surveillance mechanisms such as the interception of private communications. Thus, even if there is a mistaken in the processed data, the subject cannot exercise rights since they are not aware that the information is being processed in cases of national security or law enforcement. A different situation exists when the information is directly obtained by an individual. In such cases, the individuals may exercise their rights to access, rectification, cancelation or objection (ARCO) under the data protection laws*."
[146] Interview conducted on 3 March 2023 with a representative from a leading Mexican law firm.
[147] Interview conducted on 2 March with a representative from a leading Mexican law firm. This was further confirmed in an interview conducted on 8 March 2023 with a representative from a public research institution.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

2.1.2.2 INTELLIGENCE ACTIVITIES AND NATIONAL SECURITY

All actions and authorities for the purpose of preserving the national security in Mexico must comply with the National Security Law (NSL)[148]. The legal rules also establish how the different entities, local and federal, can collaborate for this purpose. The law establishes that personal data processed by national security authorities in Mexico in order to establish or prevent a national security threat is confidential governmental information[149]. Confidential information can only be accessed in a limited manner by individuals.

Throughout the development of intelligence activities[150], the authorised public authorities may use any means of collection of information, if the individual freedoms and human rights are observed[151]. Additionally, public servants involved in activities related to national security must observe the following principles even though they are not defined in the NSL[152]:

- the legality principle;
- responsibility;
- respect for fundamental rights;
- confidentiality
- loyalty;
- transparency;
- efficiency; and
- coordination and cooperation.

Intelligence activities shall always observe the purposes of national security while preserving the democratic State[153]. As illustrated by a national expert, "*national security is a legal reason for mitigating fundamental rights. However, this mitigation is limited, the principles of legality and proportionality must be observed. The analysis of possibility of mitigation is evaluated case by case*"[154].

Intelligence agencies can perform interception of communications[155]. A judicial warrant is needed for said surveillance measure[156] and this will only happen in cases of imminent threat to national security[157]. To oversee this procedure, the competent Court can request information about the measure at any moment and will also determine for how long the surveillance can take place[158]. The information gathered through this procedure cannot be used as evidence in administrative or judicial procedures. Intervention of private communication for law enforcement must comply with the CNPP[159].

National security activities are overseen by the legislative power. A bicameral commission[160] is responsible for conducting the oversight. The legal provisions are generic and include the possibility to

[148] *Ley de Seguridad Nacional* (NSL).
[149] Articles 6, V and 63 of the NSL.
[150] Intelligence is defined by the NSL as "*any knowledge obtained by the collection, processing, dissemination and exploration of information, for decision-making in matter of national security*" (Article 29).
[151] Articles 31 and 61 of the NSL.
[152] Article 61 of the NSL.
[153] Article 3 of the NSL.
[154] Interview conducted on 8 March 2023 with a representative from a public research institution.
[155] According to Article 39 of the NSL, the interception can apply to "*private communications and emissions, made through any transmission mean, already known or to be known, including images recordings*".
[156] Even in urgent cases, as established by Article 49 of the NSL "*In exceptional cases, when compliance with the procedure established in the Section II of this Chapter compromises the success of an investigation and there are indications that a threat to National Security may be consummated, the judge, due to urgency, may authorise immediately [the interception] as required*".
[157] Articles 34 and 35 of the NSL.
[158] The intervention can last up to 180 days. This timeline can be renewed for the same period by another judicial order, as long as there are reasons for that (Articles 43 and 44 of the NSL).
[159] Article 36 of the NSL.
[160] With three Senators and three deputies.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

request information from the authorities involved in the national security activities and evaluate reports about such actions[161]. However, such a report can be broad and there are no specific legal requirements about the content of these documents[162]. Such dossiers will also omit any information that affects national security and activities for such purposes or the privacy of individuals. This is because no registry shared with the oversight body should contain confidential information[163].

The NSL also establishes that the oversight and the execution[164] of interventions for national security purposes are the responsibilities of the Centre of Investigation and National Security[165] *(Centro de Investigación y Seguridad Nacional* - CISEN, in the Spanish acronym). In 2018, the CISEN was substituted by the National Centre of Intelligence (*Centro Nacional de Inteligencia - CNI*, in the Spanish acronym).

The CNI is an autonomous and decentralised body[166]. Thus, there are legal provisions about the internal oversight of national securities activities. In cases not addressed by the NSL, judiciary oversight shall be observed, and the Federal Code of Civil Procedures and the Organic Law of the Judiciary Power of the Federation will prevail and must be followed[167]. In gap scenarios involving the principle of transparency, the General Law for Transparency and Access to Public Data shall be considered, and, in these exceptions the INAI can act in overseeing the activities.

Following the legal obligations related to personal data, the CNI has published its privacy notice[168]. This document, however, only addresses the personal data processed to control the access of the building. Together with the privacy notice, the CNI published a guide on how to exercise the ARCO rights before the CNI[169]. On this opportunity, the CNI clarified that if a legal provision blocks these rights, it will not respond to the requests. It is important to note that the responses to said requests can be reviewed by the INAI, since the CNI is a federal body. The data protection documents, however, reaffirm that data processing for national purposes is an exception to the rules set out by the LGPDSSO and even to the constitutional rights to data protection. Thus, even though the LGPDSSO is a more recent law, it does not seem that it affects the provisions of the NSL. Academic research has shown that citizens' requests to national security agencies for access to data tend not to be fully responded to[170].

2.1.2.3 OVERSIGHT MECHANISMS

This section describes the oversight and redress mechanisms for the public and private sector excluding national security activities. The oversight and redress mechanisms for national security activities were described at the end of the previous section 2.1.2.2 on intelligence activities.

[161] Article 57 of the NSL.
[162] Article 58 of the NSL establishes that "*In the months in which the regular sessions of the Congress begin, the Technical Secretary of Council [of National Security] must render to the Bicameral Commission a general report of the activities carried out in the immediately preceding semester. The Bicameral Commission may summon the Technical Secretary to explain the content of the report*."
[163] Article 59 of the NSL.
[164] One of the attributions of the Centre is to "*operate intelligence tasks as part of the national security system that contribute to preserving the integrity, stability, and permanence of the Mexican State, to support governance and to strengthen the rule of law*" (Article 19, I NSL).
[165] Article 41, NSL.
[166] Article 18, NSL.
[167] Article 8, III, NSL.
[168] CNI, *Aviso de Privacidad Integral*, available at: http://www.cni.gob mx/transparencia/docs/Aviso-Privacidad-Integral.pdf.
[169] CNI, *Guía para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposicioón de datos personales*, available at: http://www.cni.gob.mx/transparencia/docs/Guia-ARCO.pdf.
[170] López, L. C. J., 'Seguridad nactional, inteligencia militar y acceso a la información en México', *URVIO Revista Latinoamericana de Estudios de Seguridad*, no. 21, 2017, available at: http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-42992017000100140&script=sci_arttext.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

For the public sectors, different actors are tasked with providing oversight. Considering the system set by the LGPDSSO and the LGTAIP, each federal entity must have a competent authority to oversee data protection, data access and the transparency rules. The INAI is the federal authority and each state and the Federal District come with a local authority.

Each local oversight authority[171] is the first instance for oversight over activities of public authorities. Thus, if a municipal or state public authority has an action challenged by an individual, this matter should be taken first to the local oversight authority. In the same sense, if the challenged action is made by a federal public authority, the INAI is the body responsible for oversight. However, the INAI can also be considered as a second instance, since it is an autonomous body that oversees the activities of the regional authorities. The oversight activities developed by the INAI can start either *ex officio* or be based on a complaint[172].

In any case, decisions by the oversight authorities can be challenged judicially. Federal judicial courts can overturn the delivered decisions of the specialised bodies, acting as the last instance of the oversight system. Also, the Supreme Court can be called upon to decide in disputes, especially considering that data protection is a fundamental constitutional right.

For the private sector, the INAI's role of overseeing the enforcement of the LFPDSSPP may occur by the initiative of the own authority or by a petition of a party. In case a private party does not observe the legal provisions[173], the INAI may initiate a procedure to apply sanctions, especially fines. Provoking a data breach for profit is considered a crime. Processing personal data accessed after an error of the data subject or of a third party is also considered to be a crime[174].

2.1.3 DATA SUBJECT RIGHTS

2.1.3.1 AVAILABLE RIGHTS AND THEIR SCOPE OF APPLICATION

The constitutional rights are reinforced by the specific Mexican laws on data protection (LFPDSSPP and LGPDSSO). Considering the constitutional aspects of data protection, both laws apply to any person, regardless of their nationality, if they follow the respective procedure.

Article 22 of the LFPDSSPP stipulates that any person – or their legal representative – may exercise, at any time, the right to access, correction, objection, and opposition (*derechos* ARCO). Limits exist for the exercise of those rights. Correction may only occur when the data is incorrect or incomplete[175]. The right to objection is limited, since the controller is not obliged to exclude the information when there is a legal exception, which includes following a legal obligation[176] and to act in the public interest[177]. The right to access data is also related to the transparency rules set by the LGTAIP. This law establishes that the request to data access is free of charge, which can change in cases of requests of reproduction or delivery of the data[178]. Requests can receive a positive or negative response by an authority. These responses, can, as explained above in section 2.1.2.1, be reviewed by the competent authorities via revision claims.

[171] Considering that each Mexican jurisdiction must have a specific and local authority to oversee the activities of transparency and data protection.
[172] INAI, *Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, available at: https://home.inai.org mx/wp-content/documentos/DocumentosSectorPublico/_GuiaPrincipiosDeberes.pdf.
[173] Article 59 of the LGPDSSPP.
[174] Articles 67 and 68 of the LGPDSSPP.
[175] Article 25 of the LGPDSSPP.
[176] Article 26, II of the LGPDSSPP.
[177] Article 26, V of the LGPDSSPP.
[178] Article 17 of the LGTAIP.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Requests to exercise data subject's rights may be denied in cases where (i) the request was sent by someone other than the data subject who is not credited as a legal representative; (ii) the personal data are not part of the databases of the company[179]; (iii) the rights of a third party are affected; (iv) the request has already been addressed; or (v) there is a decision of a competent authority limiting said rights[180].

The controller must provide an answer to the data subject within 20 days and in case of complying with the request, the controller must solve the question in the following 15 days. However, when private companies are responsible for the processing of personal data, some internationally recognised subjects' rights do not apply, since there are no provisions regarding the right to be forgotten, the right to restrict processing and the right to data portability.

The INAI is responsible for assuring the compliance of private parties with the LFPDSSPP, which includes the oversight of auto-regulatory practices – codes of good practices, that should facilitate the exercise of rights – alongside sectorial authorities[181].

Similar provisions apply to the public sector[182]. However, some differences apply. For instance, the complaints must be targeted to the competent authority, which include regional oversight bodies. As explained in section 2.1.2.2 above, the system for data protection in the public sector relies on the actions of different authorities. The INAI is responsible for the oversight of data processing activities of federal bodies, including bodies working for national security purposes. State and municipal public authorities have their processing activities overseen by local authorities. Thus, in cases where the data subject does not agree with the response to their requests, the individual can first complain to the local authority.

Regarding the right to objection, the data subject can request the exclusion of their personal data from archives, registries, and other systems[183], explaining the reasons behind the request[184]. However, there are limitations to this exercise. For instance, telecommunication companies must keep information for 90 days. According to this legal provision, the data subject cannot object to this retention of data, since the processing is necessary for a legal obligation.

A data subject can also oppose or cancel any processing that may cause any harm to him or her. This provision includes automated processing that may affect the interest, rights, and freedoms of data subjects, if there is no human participation and the purpose of this activity is profiling the subject. A data subject must identify the risks or harms of the processing[185].

The right to portability applies to data controlled by public authorities. Upon request, the public authority shall provide a copy of the personal data controlled by the body. The information must be in an interoperable electronic format[186].

Beyond the possibilities set by the LFPDSSPP, public authorities may also reject requests under different circumstances[187]. Thus, public authorities can deny requests that might harm judicial or administrative activities or that are directed to a public body that is not competent. Data processing can continue when necessary to protect legitimate interests or to comply with legal obligations of the subject,

[179] In this case, the request should be directed to the controller of the personal data.
[180] Article 34 of the LGPDSSPP.
[181] Articles 43 and 44 of the LGPDSSPP.
[182] Third tile – Data subjects rights and exercise – of the LGPDSSO.
[183] Article 46 of the LGPDSSO.
[184] Article 52, Paragraph 5 of the LGPDSSO.
[185] Article 52, Paragraph 6 of the LGPDSSO.
[186] Article 57 of the LGPDSSO.
[187] Article 55 of the LGPDSSO.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

and when the maintenance of the Mexican state relies on this activity. The requests can also be denied when the data is related to the financial oversight duties of the subject[188].

After receiving the request, the public authority has up to 20 days to respond. This period can be amplified up to 10 more days if the data subject is notified. In case of a positive response to the request, the public body also has 15 days to apply the desired measure[189].

When the data subject is not satisfied by the solutions provided by the regional oversight body, they can ask for review at the INAI. However, the Mexican Supreme Court of Justice ruled that constitutional matters cannot be solved by the INAI when the competence is held by the higher court[190]. Another decision by the Mexican Supreme Court established that when judicial bodies are deciding about matters related to the INAI's competences, the courts do not have to limit their analysis to what was already established by the INAI[191].

Data breaches in the public sector require actions of the authorities. The controller must present an action plan to guarantee the protection of the data, analysing the plausible causes of the vulnerability. The public authority must immediately notify the data subject. Whenever the violation can substantively affect rights, the INAI should also be notified[192].

As highlighted by lawyers, the systems set up for the public and private sector are very similar. However, data subjects have more difficulties in enforcing their rights under public authorities. A national expert believes the opposite applies, especially considering that the majority of data protection procedures are set in big Mexican cities, where the most structured public entities are also established.

Finally, it is essential to remember that the ARCO rights are fundamental rights, constitutionally protected[193]. As a result, they should be complied with in every data-processing activity, regardless of the nationality of the subject. Observing the purposes of the processing, the ARCO rights can only be mitigated when the measure is proportional and necessary. In specific cases, special legislation should also be taken into account. When data is processed for law enforcement purposes, the National Criminal Procedures Code applies. In the framework of national security activities, the NSL applies. However, specialists confirmed that there are no specific legal provisions about the right to be informed of being the target of surveillance measures once they are concluded, as also detailed in section 2.1.3.1. According to the interviewed national experts, subjects "*are not aware that their information is being processed in cases of national security or law enforcement access*"[194].

2.1.3.2 REDRESS MECHANISMS

In the private sector, once a data subject receives a response to a request to exercise data protection rights from a private controller or the period of response is over, the individual has 15 days to submit a complaint to INAI[195]. After receiving the complaint, the INAI receives and gathers evidence to then resolve the request within 50 days - that can be extended to 100 days[196] - which may include

[188] See further Articles 52 and 55 of the LGPDSSO. The INAI has not published any specific guideline further clarifying when such situations occur.
[189] Article 51 of the LGPDSSO.
[190] Case 2024641 of the Supreme Court of Justice of May of 2022, Thesis 2a./J. 23.2022 (11a)..
[191] Case n. 2011608 of the Supreme Court of Justice of May of 2016, Thesis 2a. XIX/2016 (10a)...
[192] Article 40 of the LGPDSSO: "*The controller shall promptly inform the data subject, and as applicable, the INAI and the local oversight bodies, of any breaches that significantly affect rights, as soon as it is confirmed that the breach has occurred and that the controller has begun to take actions aimed at triggering an exhaustive review process of the magnitude of the breach, so that the affected data subjects may take the corresponding measures to defend their rights".*
[193] Article 16, Constitution.
[194] Interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.
[195] Article 45 of the LGPDSSPP.
[196] Article 47 of the LGPDSSPP.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

reconciliation between the parties. In case of a positive outcome for the data subject, the controller has 10 days to comply with the request. When another competent court is following a procedure that might modify or revoke INAI's decision, the national authority may conclude that the complaint is inadmissible[197]. Following the INAI's decision of the complaint, the parties may request the annulment of the decision to the Federal Court of Fiscal and Administrative Justice (*Tribunal Federal de Justicia Fiscal y Administrativa*)[198].

The national experts interviewed noted that the judicial courts tend not to take into account the guidelines issued by the INAI. This has to do with the fact that Supreme Court has determined that these documents are non-binding[199].

Besides the complaints related to the exercise of data protection rights, data subjects may also ask for compensation when they consider that there was any harm to their goods or rights, according to specific norms[200], including the civil legislation of liability.

There are different options for redress against actions by public authorities as elaborated upon by one of the interviewed experts[201]. As a rule, when individuals have a complaint about the compliance of any action with data protection rules, they should address it first to the public authority, as the author of the activity, first. If the individuals concerned still disagree with the response - or there is a lack thereof, they can then lodge a complaint to the oversight authorities. In case of federal bodies this will be directed to the INAI. For activities of municipal or state authorities, the complaint should be directed to the local oversight authorities. After a resolution of a complaint by a local authority, the dispute can still be forwarded to the INAI as a second instance. These processes follow the general administrative procedural rules. Where the non-compliance with data protection rules also constitutes a crime, the individual or the Prosecutor's Office in charge can go directly to the court system, following the criminal procedure rules. As reported by one of the interviewed experts, in one instance, the INAI has brought a data protection incident that was a potential criminal act to the attention of the competent authority[202]. However, in this case, as explained by the interviewed national expert, this happened based on the general duty of every person to report crimes, not because of any formal cooperation[203]. The INAI has no formal powers to bring cases to court. Judicial bodies can also be involved in disputes regarding data protection when authorities use the information beyond judicial orders or when there is an abusive request to access confidential information.

2.1.4 OVERVIEW OF RELEVANT LEGISLATION

Public authority activity	Laws applied	Oversight	Redress mechanisms
National Security	National Security Law	Legislative bodies	N/A
Law enforcement purposes	Criminal Procedures Code LGPDSSO	Judiciary INAI	Judiciary
General rules of data access	LGPDSSO LGPDSSP Local legislations	INAI	INAI Judiciary

[197] Article 52, III of the LGPDSSPP.
[198] Article 56 of the LGPDSSPP.
[199] Interview conducted on 8 March 2023 with a representative from a public research institution. A similar remark was made in an interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.
[200] Article 58 of the LGPDSSPP.
[201] Interview conducted on 8 March 2023 with a representative from a public research institution.
[202] Interview conducted on 2 March 2023 with a representative from a leading Mexican law firm.
[203] Ibid.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

2.2 TÜRKIYE

2.2.1 RULE OF LAW, RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

2.2.1.1 CONTEXT AND CONSTITUTIONAL LAW

Türkiye is a constitutional republic with a presidential representative democracy. Similar to most EU Member States, the legal system in Türkiye is based on civil law with codified laws[204]. According to Article 2 of the Turkish Constitution, the Republic of Türkiye is a "*democratic, secular and social state governed by rule of law*"[205]. Following a referendum held on 16 April 2017, fundamental changes to the governing structure were introduced by exchanging the long-standing parliamentary system with a *sui generis* quasi-presidential system. Hence, the Constitution underwent considerable amendments with the new system becoming effective as of 9 July 2018. In principle, the Constitution provides a separation of powers (i.e., legislative, executive and judicial) between the parliament[206], the president (the head of state and head of government)[207], and the judiciary[208].

Türkiye is a founding member of the United Nations and has been a member of the Council of Europe (CoE) since 13 April 1950. Since December 1999, Türkiye has been an EU candidate country and accession negotiations started in 2005 but have not advanced recently. Moreover, Türkiye and the EU have been expanding their economic and trade relations since 1963, through the Ankara Association Agreement, and a Customs Union which was established in 1995.

In terms of international obligations, Türkiye signed and ratified the European Convention of Human Rights (ECHR) in 1954, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), as well as the UN's International Covenant on Civil and Political Rights. However, the updated version of the Convention 108 on protection of individuals with regard to the Processing of Personal Data (Convention 108+) is yet to be signed and ratified[209]. By signing and ratifying the above documents, Türkiye commits to the protection of human rights, including the right to privacy and data protection.
Since December 2022, Türkiye has also been party to the Organisation for Economic Co-operation and Development (OECD) intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes[210].

[204] Case law is also taken into consideration for the interpretation of laws.
[205] Excerpted from the official English translation of the Constitution of the Republic of Türkiye provided by Grand National Assembly of Türkiye (GNAT), May 2019, available at: https://www5.tbmm.gov.tr/yayinlar/2021/TC_Anayasasi_ve_TBMM_Ic_Tuzugu_Ingilizce.pdf.
[206] Article 7 of the Constitution of Türkiye: "*Legislative power is vested in the Grand National Assembly of Türkiye on behalf of Nation. This power shall not be delegated*."
[207] Article 8 of the Constitution of Türkiye: "*Executive power and function shall be exercised and carried out by the President of the Republic in conformity with the Constitution and laws*."
[208] See Chapter 3 *"Judicial Power*", Articles 138-160 of the Constitution of Türkiye.
[209] It is important to highlight that an international agreement duly approved and enacted by the legislature is also deemed to be part of the legal system and Article 90(5) of the Constitution privileges international agreements related to fundamental rights and stipulates that *"International agreements duly put into effect have the force of law. In the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail."*, see Article 90(5) of the Constitution.
[210] OECD, *Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access*, available at: https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm#.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

The Constitution of Türkiye[211] includes protection for several basic human rights and freedoms such as the right to privacy[212], freedom of communication[213], and freedom of expression[214]. The Constitution also introduces certain guarantees and conditions for the limitations of those rights[215]. In particular, Article 13 stipulates that fundamental rights and liberties may be limited only by law[216] and for the reasons specified in the relevant Articles of the Constitution, without prejudicing their essence. These restrictions must not be contrary to requirements of the democratic order of society and the secular republic, as well as the proportionality principle. Additionally, Article 16 of the Constitution of Türkiye stipulates that *"The fundamental rights and freedoms in respect to aliens may be restricted by law compatible with international law."* Article 20 of the Constitution of Türkiye guarantees privacy and data protection rights to everyone and further introduces restrictions to the state's interference with the processing and recording of such data in line with the ECHR[217]. Furthermore, this provision also entitles individuals to the right to be informed, the right of access and the right to request correction and deletion of their personal data.

2.2.1.2 THE HUMAN RIGHTS SITUATION IN TÜRKIYE

There are serious deficiencies in the protection of fundamental rights and functioning of Türkiye's democratic institutions. Türkiye had the most registered violations of human rights of the ECHR, with a total of 3 900 judgments of the European Court of Human Rights (ECtHR) in the period 1959-2022[218]. A report of the EU highlighted the fact that although human and fundamental rights are enshrined in the Turkish Constitution and legislations, a "serious backsliding" in terms of the rule of law and human rights is the reality[219]. As of December 2022, 20 100 applications against Türkiye were pending before the ECtHR[220]. Türkiye has been found to have violated the right to respect for private and family life 140 times by the ECtHR during the period 1959-2022. In light of this, the CoE condemned the human rights situation in Türkiye and repeatedly criticised it for not complying with the ECHR. In February 2022, the CoE agreed on developing further restrictive measures in response to the serious violations of human rights in Türkiye and non-compliance with ECtHR decisions[221].

[211] Articles 17 to 40 of the Constitution of Türkiye.
[212] Article 20 of the Constitution of Türkiye.
[213] Article 22 of the Constitution of Türkiye.
[214] Article 26 of the Constitution of Türkiye.
[215] Articles 13, 14 and 15 of the Constitution of Türkiye introduce safeguards and conditions to the limitations of human rights.
[216] It is important to underline that the concept of law in this sense corresponds to an act that is formally adopted by the Grand National Assembly of Türkiye by excluding executive or secondary legal instruments to restrict fundamental rights. Thus, the Constitution take stricter approach to the restriction of fundamental rights.
[217] Following the amendments of 2010, Article 20 of the Constitution of Türkiye: "*Everyone has the right to demand respect for his/her private and family life. Privacy of private or family life shall not be violated*".
[218] As of December 2022, Türkiye has been found to violate the right to life (Article 2 ECHR) 143 times, and lack of effective investigation (Article 2 ECHR) 225 times, the right to inhumane or degrading treatment (Article 3 ECHR) 348 times, and lack of effective investigation to (Article 3 ECHR) 229 times, the right to liberty and security (Article 5 ECHR) 843 times, the right to a fair trial (Article 6 ECHR) 991 times, right to respect for private and family life (Article 8 ECHR) 140 times, freedom of expression (Article 10 ECHR) 426 times and the right to an effective remedy (Article 13 ECHR) 283 times. Other important rights are for example freedom of thought, conscience and religion (Article 9 ECHR): 13 times, freedom of assembly and association (Article 11 ECHR): 117 times, prohibition of discrimination (Article 14 ECHR): 20 times. All statistics are from the Council of Europe, viewed 12 February 2023, available at: https://www.echr.coe.int/Documents/Stats_violation_1959_2022_ENG.pdf.
[219] EU Commission, *Türkiye 2022 Report*, available at: https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrkiye%20Report%202022.pdf.
[220] CoE, *European Court of Human Rights, Annual Report 2022*, p. 142, available at: https://www.echr.coe.int/Documents/Annual_report_2022_ENG.pdf.
[221] Human Rights Watch, *Council of Europe Sanctions Turkey*, available at: https://www hrw.org/news/2021/12/03/council-europe-sanctions-Türkiye . See also the decision taken by CoE, see Concil of Europe, *Interim Resolution on Execution of the judgment of the European Court of Human Rights Kavala against Turkey*, available at: https://rm.coe.int/0900001680a4b3d4.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Similarly, the EU raised several concerns regarding the deterioration of the rule of law and fundamental rights[222] in Türkiye, which have brought the accession negotiations almost to a standstill[223]. One of the concerns is the systemic lack of independence of the judiciary and the undue pressure on judges and prosecutors by the government. As stated in the most recent progress report of the EU on Türkiye the serious backsliding observed since 2016 as a consequence of the failed coup attempt is continuing. The report also highlights that despite the lifting of the state of emergency in July 2018, presidential decrees issued during the state of emergency following the failed coup attempt continue to have severe implications on fundamental rights[224]. In this regard, the United Nations Human Rights Council (the HRC) and the CoE Venice Commission called Türkiye to limit the duration and the scope of far-reaching emergency decrees and to introduce provisions for adequate judicial review[225].

NGOs such as Amnesty International and Human Rights Watch (HRW)[226] also reported that despite the newly proposed human rights' action plans and judicial reform packages, serious flaws in the judicial system persists. As a consequence, opposition politicians, journalists, human rights defenders, and others have been subjected to illegitimate investigations, prosecutions, and convictions[227]. With regard to counter-terrorism and human rights, the HRW notes that the counter-terrorism law in Türkiye is rather broad and vague which allows it to be used for politically motivated prosecutions of dissidents in particular for alleged "membership of a terrorist organisation[228]"[229].

When it comes to organisations specialised in privacy and data protection rights, Privacy International has raised concerns about the lack of safeguards against public and private surveillance in Türkiye, which were also observed in relation to the investigations initiated after the failed coup attempt[230] and COVID-19 tracking[231].

In Türkiye, there are a variety of data retention requirements imposed upon private companies. For instance, the mandatory retention of traffic data is imposed upon telecommunication service providers

[222] For example, it is noted that Türkiye withdrew from the CoE Istanbul Convention-on preventing and combating violence against women and domestic violence, draw severe criticisms from several NGOs and international organisations. See EU Commission, *Türkiye 2022 Report*, p. 141, available at: https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrkiye%20Report%202022.pdf .

[223] EU Commission, *Türkiye 2022 Report*, p. 5, available at: https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrkiye%20Report%202022.pdf .

[224] See EU Commission, *Türkiye 2022 Report*, p. 5, p. 4: "*Some legal provisions granting government officials extraordinary powers and retaining several of the restrictive elements of the state of emergency remained integrated into law, which continued to have a significant impact on democracy and fundamental rights."* also echoed in the report of 2020 and 2021. See also "*Under the state of emergency, Turkey derogated from its obligations under the European Convention on Human Rights and the International Covenant on Civil and Political Rights. When the state of emergency ended, all derogations were revoked but Parliament has permanently adopted most of the 36 statutory decrees issued under the state of emergency.*", available at: https://www.gov.uk/government/publications/turkey-country-policy-and-information-notes/country-policy-and-information-note-gulenist-movement-turkey-february-2022-accessible-version.

[225] European Commission for Democracy Through Law (Venice Commission), *Draft Opinion on the Provisions of the Emergency Decree Law N° 674 Of 1 September 2016 Which Concern the Exercise of Local Democracy In Türkiye*, p. 21, available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2017)021-e.

[226] Human Rights Watch (2022), *Word Report Türkiye Chapter*, available at: https://www.hrw.org/world-report/2022/country-chapters/Türkiye.

[227] Amnesty International, *Report 2021/2022*, p. 371.

[228] In the similar vein, the United Nations High Commissioner for Human Rights (OHCHR) also raised concerns over the enjoyment of the right to fair trial and access to justice while a pattern of persecution of lawyers representing individuals accused of terrorism is observed. See The United Nations Human Rights Council Working Group on the Universal Periodic Review, *Compilation on Türkiye Report of the Office of the United Nations High Commissioner for Human Rights*, , 20–31 January 2020, p. 5.

[229] Ibid, p. 6.

[230] Statewatch, *Algorithmic persecution in Turkey's post-coup crackdown: The FETÖ-Meter system*, 25 November 2021.

[231] Privacy International (2015), *The Right to Privacy in Türkiye*, available at: https://privacyinternational.org/sites/default/files/2017-12/UPR_Türkiye_0.pdf, and Privacy International search on Türkiye, available at: https://privacyinternational.org/examples/3728/Türkiye -prepares-comprehensive-quarantine-surveillance.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

by the Authorisation Regulation on the Electronic Communication Sector[232]. This Regulation aims to determine the procedures and principles for authorisation regarding electronic communication services, networks and infrastructures. Article 16 of the Regulation imposes a number of requirements on electronic communication service providers. The mandatory retention of traffic data is one of these responsibilities under Article 16(1)(f). According to this provision, access providers or the operators providing the telephone service are obliged to retain the following data for two years: the IP address of the parties, the port range, the start and end time of the service provided, the type of service used, the amount of data transferred, the traffic information of the calls made over their infrastructure. A prominent case of mass surveillance concerns the Centralized Monitoring System that is managed via Information and Communication Technologies Authority (ICTA), known as "*Bilgi Teknolojileri ve İletişim Kurumu*" (BTK), and enables the monitoring of all phone and internet communications. In 2020, it was alleged by a Member of the Grand National Assembly of Türkiye that the BTK requested internet service providers to send internet traffic records of all users (e.g., name, surname of the subscriber, IP numbers, location data) to it hourly by providing a detailed technical document about the requested type and format of the data[233]. HRW notes that widely used social media platforms [redacted] have complied with a 2020 legal amendment requiring them to establish offices in Türkiye, raising concerns that they will be forced to increase their compliance with government censorship in the future in order to avoid heavy fines and other penalties[234].

2.2.1.3 PERSONAL DATA PROTECTION IN TÜRKIYE

Apart from the overarching protection provided to privacy and personal data of individuals in the Turkish Constitution, there are other laws which provide specific, sometimes context-dependent, protection measures. For example, the Turkish Criminal Law numbered 5204 (TCL) punishes certain misuses of personal data and brings dissuasive penalties under Article 134 (violation of privacy and secrecy), Article 135 (illegal recording of data, violation of data collection law, data collection without consent), 136 (illegal transfer and dissemination of personal data) and 138 (non-destruction of data). The Turkish Personal Data Protection Law (TPDPL)[235] applies since 7 April 2016. Consequently, certain personal data processing operations are subject to the obligations and safeguards arising from the TPDPL. Article 4 TPDPL obliges data controllers and processors to comply with specific data protection principles such as lawfulness, accuracy, purpose and storage limitation, which align with the data protection principles enshrined in Article 5 GDPR. Furthermore, Article 11 TPDPL entitles data subjects to specific data subject rights including but not limited to the ones referred to in the Article 20 of the Constitution, namely the right to object to automated decision-making and the right to information about any international transfers of the data.

The TPDPL establishes the Personal Data Protection Supervisory Authority (SA) as a public independent institution by ensuring its financial and administrative autonomy in Article 19 and defines a set of general duties under Article 20.[236] Moreover, the Personal Data Protection Board (the Board),

[232] The similar obligation is imposed upon internet access providers and hosting service providers. For the access service provider, the duration of traffic data is one year in Article 15(1)(b) of Regulation on Procedures and Principles Relating to Authorization to Access Providers and Hosting Providers. For hosting service provider the mandatory retention is six months (Article 16(1)(c) of the same Regulation), available at: https://www.mevzuat.gov.tr/anasayfa/MevzuatFihristDetayIframe?MevzuatTur=7&MevzuatNo=11679&MevzuatTertip=5.

[233] See, Medyascope, *BTK-gate: Internet activity, identity, and personal data of all users in Turkey has been collected by BTK for the past year and a half*, available at: https://medyascope.tv/2022/07/21/btk-gate-internet-activity-identity-and-personal-data-of-all-users-in-Türkiye -has-been-collected-by-btk-for-the-past-year-and-a-half/.

[234] Human Rights Watch, *Turkey: YouTube Precedent Threatens Free Expression*, available at: https://www.hrw.org/news/2020/12/19/turkey-youtube-precedent-threatens-free-expression.

[235] The Turkish Personal Data Protection Law (TPDPL), numbered 6698, English version, available at: https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law.

[236] See, the Activity report for 2017-2022 published by the Turkish SA, "5. *yılında Kişisel Verileri Koruma Kurumu*", 23 November 2022, available at: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/b5731c6c-540b-45eb-a2d8-d7cef57cf197.pdf.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

which is the decision-making body of the SA, was established pursuant to Article 21[237]. Among other duties and powers, the Board can issue administrative fines based on the criteria set in Article 18 in cases where the TPDPL is violated. However, the framework that establishes the Turkish SA and the Board has been criticised in EU progress reports due to a lack of safeguards for their respective independence[238]. In order to comply with the EU acquis, amendments to the TPDPL were proposed by the Turkish SA and legislative procedures are still ongoing at the time of drafting this report.

With respect to international personal data transfer, Article 9 TPDPL sets criteria for the transfer of personal data to countries outside of Türkiye and brings additional obligations for data controllers and processors. The TPDPL allows international personal data transfer in three instances (i) obtaining the explicit consent of the data subject; (ii) the country to which personal data will be sent has an adequate level of protection[239]; or (iii) in case, adequate protection is not provided, the data controllers in Türkiye and in the target country undertake such protection with an agreement in writing and obtain the approval of the Board[240]. At the time of writing this report, no country with adequate protection has so far been designated by the Turkish SA. Since the adoption of the TPDPL, the Turkish SA has published a number of information notes to provide further guidance on several aspects related to the application of TPDPL, including the international personal data transfer together with legal documents related to the model contractual clauses and binding corporate rules (BCR)[241]. In 2018, the Turkish SA published two model clauses, similar to the standard contractual clauses (SCCs) under the GDPR, one for data transfers from a data controller to data controller, and one from a data controller to a data processor[242]. However, unlike the GDPR, the TPDPL obliges data controllers to seek approval from the Board after they conclude the model clauses in order to have a valid legal basis for international data transfer[243]. Moreover, as announced by the Scientific Committee working on amendments of the TPDPL, the international personal data transfer rules will be updated in line with the GDPR rules[244]. For the moment, there is little official information available online about the scope and present status of the proposed TPDPL modifications.

Although the TPDPL provides specific safeguards for personal data processing in Türkiye, according to exceptions in the law, personal data could be processed and stored if it was a matter of national security. As such, Article 28 TPDPL excludes the law enforcement and national security domain from its scope together with the "*personal data (that) are processed by judicial authorities or execution authorities regarding investigation, prosecution, judicial or execution proceedings*". An action for the annulment of some Articles including the provision of Article 28 TPDPL was filed with the Constitutional Court. The Constitutional Court rejected the action and found that the processing of personal data within the scope of preventive, protective and intelligence activities regulated in subparagraph (ç) of Article 28

[237] According to the Article 22 TPDPL, the Board consists of nine members, of which five shall be elected by the Grand National Assembly of Türkiye; four members shall be elected by the President of the Republic of Türkiye with certain election procedures.
[238] The EU Progress Report 2022 states that the lack of compliance of personal data protection rules with the acquis is an obstacle to data sharing and co-operation in many areas, in particular, in the context of Europol and Eurojust, p. 32.
[239] Pursuant to Article 9(3) TPDPL, the Board shall declare the countries having adequate level of protection.
[240] Article 9 TPDPL.
[241] See with regard to notes published by the Authority on *International Data Transfer*, available at: https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim, https://www kvkk.gov.tr/Icerik/4106/Kisisel-Verilerin-Yurtdisina-Aktarilmasi, https://www kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim, and https://kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU.
[242] See, The Turkish SA, *Yurtdısına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhutnamede Yer Alacak Asgari Unsurlar*, 2018, available at: https://kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-VeriSorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-AsgariUnsurlar.
[243] See, The Turkish SA, *Bağlayıcı Şirket Kuralları Hakkında Kamuoyu Duyurusu*, 10 April 2020, available at: https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU.
[244] See, Presidency of Türkiye, *Human Rights Action Plan (2021-2023)*, Circular 2021/9, available at: https://insanhaklarieylemplani.adalet.gov.tr/resimler/%C4%B0nsan_Haklar%C4%B1_Eylem_Plan%C4%B1_ve_Uygulama_Takvimi.pdf.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

TPDPL is in accordance with the Constitution while certain safeguards against those activities are envisaged in other specific laws[245].

It can be argued that although there are certain safeguards provided in different laws, the safeguards against the interference with privacy and data protection rights are rather fragmented[246], as will be further explored in the following section[247]. It is important to note that Turkish law does not regulate law enforcement use of data in a similar manner to how it is regulated in the EU by the Law Enforcement Directive. There is thus no separate legal instrument on personal data processing by law enforcement authorities[248]. However, in addition of the guarantees for privacy and data protection rights provided by the Constitution, certain safeguards can still be found in secondary legislation setting out the powers and duties of competent authorities (i.e. MIT Law, Police Law, Gendarmerie Law and Criminal Procedure Law), particularly, in the context of law enforcement and national security, as also further examined in detail in the next section

2.2.2 GOVERNMENTAL ACCESS TO PERSONAL DATA

2.2.2.1 GOVERNMENTAL ACCESS FOR NATIONAL SECURITY PURPOSES

There are three main intelligence organisations in Türkiye. First, the *Milli İstihbarat Teşkilatı* (MIT) (National Intelligence Organization) is responsible for providing intelligence related to national security, counter-intelligence activities and combating terrorism activities. Second, the General Directorate of Security[249], which forms part of the Ministry of Interior, is mandated to carry out intelligence activities to protect national security as well as to ensure general security and public order at the national level[250]. For this purpose, it collects and evaluates information and conveys the intelligence data to relevant public authorities[251]. Third, the Gendarmerie of General Command[252] is responsible for the intelligence activities to combat terrorism. Regarding the territorial competence of these organisations, while the MIT and the General Directorate are competent at the country level, the Gendarmerie has competence in the rural areas where there is no police force (the General Directorate). In other words, the Gendarmerie is responsible for the areas outside the municipal boundaries of provinces and districts where there is no police force[253]. In the following paragraphs, the report describes the competences and tasks of each these organisations in light of their relevance for personal data processing, underlining also any applicable safeguards, including oversight and redress mechanisms.

[245] Atli, T., *Kişisel Verilerin Önleyici, Koruyucu Ve İstihbari Faaliyetler Amaciyla İşlenmesi*, 2 Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, 2019, pp. 16-17, available at: https://dergipark.org.tr/tr/pub/neuhfd/issue/46494/579600. See also the decision of the Constitutional Court. AYM, E.2016/125., K.2017/143., Karar Tarihi: 28.09.2017 E.T: 03.05.2019, paragraphs 151-159, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2017/143?KararNo=2017%2F143.

[246] The fragmented safeguards mean the safeguards mentioned in the study. See the list of legal instruments concerning the right to privacy and data protection. Kaya, M.B. F. Tastan, *Kişisel Veri Koruma Hukuku: Mevzuat & İçtihat & Bibliyografya*, online, version 2.5, pp. 1774-1776, available at: https://mbkaya.com/kisisel-veri-koruma-hukuku-mevzuat-ictihat/.

[247] See in particular sub-sections 2.2.2.4 and 2.2.2.5.

[248] Moreover, there is also substantial ambiguity on the limits of personal data processing by law enforcement, gendarmerie or intelligence services, in particular with regard to the inadequacy of legal barriers and safeguards against a broad interpretation of national security by security agencies. Therefore, it is argued that the legal safeguards provided against security agencies are lacking clear-cut limits for the processing of personal data by such authorities. See, Ünver, H.A., Kim G., 'Data Privacy and Surveillance in Türkiye', *EDAM Cyber Policy Paper Series 2*, 2017, p. 29.

[249] Law on the Duties and Powers of Police dated 1934 and numbered 2559 (Police Law), available at: https://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf.

[250] Add. Article 7 (1) of Police Law.

[251] Add. Article 7 of Police Law.

[252] Law on the Duties and Powers of the Gendarmerie Organization dated 1983 and numbered 2803 (Gendarmerie Law), available at: https://www mevzuat.gov.tr/mevzuatmetin/1.5.2803.pdf.

[253] Article 10(1) of Gendarmerie Law.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Personal data access by the National Intelligence Organisation (MIT)

Tasks and competences of the MIT

The MIT is responsible for providing intelligence related to national security, counter-intelligence activities and combating terrorism activities. The tasks and competences of MIT are stipulated in the Law numbered 2937 on the State Intelligence Services and the National Intelligence Organization (MIT Law)[254]. Article 4 of the MIT Law explicitly determines the scope of the tasks of the MIT. Article 4(1) stipulates ten different tasks of the MIT. These tasks can be divided into five categories providing intelligence regarding: (i) the protection of national security and state security, (ii) combating terrorism[255], (iii) combating international crimes[256] and cybercrimes[257], (iv) coordinating intelligence activities with other public authorities, and (v) improving the organisational and technical capacity for the aforementioned tasks. For carrying out the tasks given to MIT, MIT is equipped with the necessary competences and powers. Article 6 of MIT Law sets forth the competences of the MIT. For the report, the following three competences and powers of MIT are relevant because it might lead to the access of personal data by the MIT: (i) the power to request information and documents from public institutions and organisations as well as private entities (Article 6(1)(b)); (ii) the power to access the databases on entry and exit of foreigners, granted visas, residence permits, work permits and deportations (Article 6(1)(f)); and (iii) access to data in communication (Article 6(1)(h)).

Regarding the power to request access to information and documents held by public entities, Article 5(1) of the MIT stipulates that all public entities are responsible for providing intelligence and information to the MIT within the scope of their respective tasks. Furthermore, Article 6(1)(b) of the MIT Law states that all public entities shall respond to MIT's requests. However, if public entities consider a request unlawful due to its excessive nature, they might refuse it on the basis of its illegality. Regarding the request for access to information and documents held by private entities, the MIT can address its request to all private entities that are established in Türkiye. The scope of the private entities that can be the subject of such requests are delineated in Article 6(1)(b). According to this paragraph, the MIT can request information, documents, data and records from institutions and organisations within the scope of the Banking Law dated 19/10/2005 and numbered 5411, as well as other legal persons and institutions without legal personality, and use their telecommunication infrastructure or data processing centres. The MIT can request access to their archives, electronic data processing centres and communication infrastructure, and may contact them. In this context, private or public entities cannot avoid the fulfilment of the request by referring to other laws that apply to these private entities. Yet, as will be discussed in section 2.2.2.3, almost all administrative actions are subject to judicial review according to Article 125 of the Constitution. Thus, the legality of the request can be challenged before the administrative courts.

Substantial and procedural conditions and safeguards for personal data access

The powers of access of the MIT can include personal data if the access is related to the activities of human intelligence and signal intelligence in particular, which can be related to a natural person. The procedural and substantial conditions that protect personal data vary depending on the type of power used.

[254] Law 2937 on The State Intelligence Services and the National Intelligence Organisation, available at: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2937&MevzuatTur=1&MevzuatTertip=5.

[255] With regard to counter-terrorism capacity and framework of Türkiye, see Council of Europe Committee on Counter-terrorism (CDCT), *Profiles on Counter-Terrorism Capacity: Türkiye*, available at: https://rm.coe.int/profile-november-2022-Türkiye/1680a94979.

[256] While there is no definition of international crimes in MIT Law, the crime of genocide (Article 76), the crime against humanity (Article 77), the crime migrant smuggling (Article 79) and of human trafficking (Article 80) are incorporated in the TCL numbered 5237 (in Turkish), available at: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5. See for the analysis of international crimes in TPC in the light of Rome Statue: Erhan, Z. (2019), *Core International Crimes In Turkish Criminal Law And The Rome Statute*, 22 Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Ankara, p. 111.

[257] Cybercrimes can be found in Articles 243- 245 of the TCL.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

For information requests to public and private entities under Article 6(1)(b), the scope of information access is restricted to the tasks of the MIT as defined in Article 4 of the MIT Law. There are no further conditions described in the MIT Law for such access, but the safeguards mentioned in the following paragraph also apply. Additional substantial and procedural conditions of information accessed by the MIT are supposed to be further specified by a regulation issued by the Presidency of Türkiye following Article 6(10) of the MIT Law. However, the regulation that specifies these conditions is not published in the official journal and is not accessible to the public in line with Article 32 of MIT Law. Nevertheless, it should be borne in mind that a restriction of fundamental rights is only possible by a law that is adopted by the Grand National Assembly of Türkiye according to Article 13 of the Constitution[258]. Thus, while the regulation might substantiate or clarify the conditions and safeguards mentioned in the MIT Law, these clarifications in the regulation adopted by the Presidency of Türkiye cannot restrict the right to data protection or other fundamental rights due to Article 13 of the Constitution.

The MIT Law provides general safeguards for situations when the MIT accesses and uses information. These safeguards apply to all measures taken by the MIT unless specifically exempted. The first safeguard is the confidentiality requirement imposed upon the MIT in Article 6(6) of the MIT Law[259]. The second safeguard is purpose limitation. Article 6(6) states that neither the record nor the information can be used for any purposes other than the tasks mentioned in Article 4 of the MIT Law[260]. Furthermore, the information possessed by the MIT cannot be requested by the Court except for crimes related to state secrets and espionage[261] according to Additional Article 1 of the MIT Law[262]. The third safeguard is that the unauthorised obtaining, stealing, faking or destruction of information or documents possessed by the MIT is criminalised in Article 27 of the MIT Law[263]. A person that commits one of the acts listed can be sentenced to imprisonment for four to ten years. If a person that is affiliated with the MIT commits such a crime, the imprisonment to be imposed is increased by up to one-third.

The access to information by the MIT has been criticised by the HRW due to the lack of protection of privacy and data protection[264]. The constitutionality of Article 6(1)(b) of the MIT Law has been assessed by the Constitutional Court of Türkiye[265] on the allegation of its incompatibility with the Constitution including Article 20 of the Constitution (right to privacy and data protection). The Court acknowledged that the powers granted to the MIT in Article 6(1)(b) constitute an interference with Article 20, which guarantees the right to privacy and right to data protection. The majority of the members of the Court found this interference (request of information access by the MIT) necessary and proportionate because there are appropriate safeguards, noting the safeguards mentioned in the previous paragraph and the internal oversight within the MIT, the ex-post oversight mechanism of the "State Supervisory

[258] Article 13 of the Turkish Constitution requires restrictions to fundamental rights to be "provided by law". This "provided by law" element is only met by a legislation adopted by the General Assembly. For instance, a presidential decree mandates the request of information and document by the MASAK (the authority responsible for combating anti-money laundering and terrorist financing). The Constitutional Court stated that it is only possible to restrict fundamental rights (right to data protection) by a legislation but not with a presidential decree. See AYM, E.2019/96, K.2022/17, 24/02/2022, paragraph 63 and following paragraphs, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/17.
[259] AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 26, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
[260] Ibid.
[261] See Articles 326-339 of the TCL.
[262] AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 27, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
[263] AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 27, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
[264] Human Rights Watch, *Türkiye Spy Agency Law Opens Door to Abuse*, available at: https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse#:~:text=(Istanbul)%20%E2%80%93%20A%20new%20law,and%20the%20right%20to%20privacy.
[265] AYM, E.2014/122, K.2015/123 T. 30/12/2015, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Council"[266] and the parliamentary oversight[267], as well as the legal redress mechanisms which will be discussed further below[268]. A dissenting opinion did not agree[269] and stated that the broad scope of power to request the information might force private entities to show incriminating evidence against themselves or their relatives or to provide information, documents, data, and records learned as a result of their profession and containing secrets such as in the context of a lawyer- client relationship[270]. In addition, the dissenting opinion underlined that the rule of law required public authorities to protect fundamental rights and freedoms when interfering with them for security purposes[271]. If the MIT is granted a broad authorisation for national security purposes, it should be foreseen that it can be used in cases directly related to the task, limited to the request, and necessary measures should be taken to protect these limits and prevent misuse[272].

Additional substantial and procedural conditions are set to limit the power in terms of access to communication data (metadata), content, and signal detection, in addition to the safeguards mentioned. The safeguards available in situations where there has been national security government access vary depending on whether the individuals that are subject of the measure are foreign or whether they are residing in Türkiye or abroad.

The following eight safeguards apply to Turkish citizens that reside in Türkiye.

- The first safeguard of a substantial nature is laid down in Article 6(2) of the MIT Law and states that access to personal data must be justified by a serious threat to national security, revealing espionage activities, preventing the disclosure of state secrets, or combating terrorism.
- The second safeguard of a procedural nature is that an order of a judge of the Assize Court in Ankara in Türkiye is required (Article 6(3) of the MIT Law). In case of urgent need, the President of the MIT or the Vice-President can order access, but the approval of a judge is required within 24 hours. If the judge does not approve the order or does not make the approval within 24 hours, then the order is deemed to be revoked.
- The third safeguard is a requirement for the order to include specific elements listed in Article 6(4). In the written order or judicial decision, the identity of the person to whom the measure will be applied, the type of communication tool, the telephone numbers, the type of measure, the scope and duration of the measure and the reasons for applying the measure have to be specified.
- The fourth safeguard in the same paragraph is the duration of the measure. The order or decision for the specific measure has to be limited to three months at one time. The measure can be extended a maximum of three times. This maximum time limit does not apply to access to content and metadata of the communication for the purpose of detecting espionage activities or combating terrorism.
- The fifth safeguard is that the measure is implemented in a specific place within the BTK or established by MIT according to Article 6(2) of MIT Law.
- The sixth safeguard is related to the destruction of the content of the communication. If the access measure is terminated, the recordings of the accessed content have to be destroyed within ten days at the latest. Affected organisations must be able to demonstrate compliance with this rule by making a report on the matter and safekeeping it so that it can be submitted in case of an audit.

[266] AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 31, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
[267] AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 32, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
[268] See Section 2.2.2.
[269] See Dissenting Opinion of Alparslan Altan and Erdal Tezcan, in particular paragraphs 1-19, AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 32, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
[270] See paragraphs 13-14 of the Dissenting Opinion of Alparslan Altan and Erdal Tezcan, AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 32, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
[271] Ibid, paragraph 18.
[272] Ibid.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

- The seventh safeguard is to record the log details of the measures in a report. The report contains the start and end time of the measures as well as the identity of the person performing the measure according to Article 6(7).
- The eighth safeguard is that if the MIT does not meet the aforementioned legal requirements while applying the measure, the evidence obtained via these measures can be considered unlawful and the persons that do not comply with these conditions can be prosecuted in accordance with the TCL according to Article 6(9) of the MIT Law.

In terms of communication data (metadata), content of communication, and signal detection for communications abroad regardless of the nationality of the affected persons or of foreigners in Türkiye, the general safeguards mentioned apply to this measure (purpose limitation, confidentiality requirement etc.)[273]. However, the specific safeguards within the MIT Law are limited in comparison with the safeguards described in the previous paragraph. To carry out its tasks in Article 4, the MIT can listen to communications or detect and evaluate signal information to obtain preventive intelligence and make an analysis with the approval of the President or Vice-President of the MIT. The necessity and proportionality requirements for this measure are not specifically mentioned in Article 6(11), though even then the necessity and proportionality requirements for fundamental rights laid down in Article 13 of the Constitution need to be respected. This was discussed in the case of *Bestami Eroğlu* by the Constitutional Court, which is further explained below[274]. The information and data processed within these activities can only be used for intelligence activities and cannot be used for other purposes including as a basis for criminal prosecutions[275].

The constitutionality of Article 6(11) of the MIT Law was assessed by the Constitutional Court of Türkiye, on the basis of an alleged violation of, among others, Article 20 (right to private life and data protection) as well as Article 22 of the Constitution (right to the confidentiality of communication)[276]. The Court found it compatible with fundamental rights by referring to the general safeguards mentioned in Article 6(1)(b)[277]. In the dissenting opinion, [redacted] some judges disagree with the majority stating that the absence of specific safeguards mentioned for Turkish citizens living in Türkiye cannot be justified and violates the right to the confidentiality of communication and refers to *Klass and other v. Germany* case of European Convention of Human Rights (ECtHR)[278]. In addition, they underline the importance of ex-ante judicial review for interference with the confidentiality of communication[279].

The Constitutional Court has assessed the legality of the personal data access by the MIT in the complaint of *Bestami Eroğlu.* This complaint was related to the access to personal data by MIT and further use by the Courts in the criminal investigation and prosecution in this specific complaint[280]. The Court explicitly stated that while the derogations from the right to data protection is possible for the purpose of national security and crime prevention, the interference with right to data protection by public authorities shall meet the legality, necessity and proportionality requirements foreseen under Article 13 of the Constitution[281]. Referring to the powers of the MIT in the paragraphs mentioned above, the Court reiterated that the MIT Law meets the legality requirement. In the specific analysis of facts, the Court

[273] AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 32, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
See the complaint of Bestami Eroğlu for the legal analysis of further process by judicial authorities in the criminal prosecution, *Bestami Eroğlu* [GK], B. no: 2018/23077, T. 17/9/2020, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/23077?BasvuruAdi=BESTAM%C4%B0+ERO%C4%9ELU.
[274] Ibid., paragraph 139.
[275] AYM, E.2014/122, K.2015/123 T. 30/12/2015, paragraph 80, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
[276] Ibid, paragraph 32.
[277] Ibid, paragraph 80.
[278] See the dissenting opinion of [redacted], AYM, E.2014/122, K.2015/123 T. 30/12/2015, available at: https://nomkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.
[279] Ibid.
[280] *Bestami Eroğlu* [GK], B. No: 2018/23077, T. 17/9/2020, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/23077?BasvuruAdi=BESTAM%C4%B0+ERO%C4%9ELU.
[281] Ibid., paragraph 145.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

analysed whether the access to personal data in the *Bylock* application[282] by the MIT and to data processed (communication data) by BTK is necessary and last recourse to pursue the aim of detecting members of terrorist organisations, which prejudices national security. The Court stated that the access to data (IP addresses, the content of message and telephone records) by deploying intelligence techniques by MIT cannot be considered as incompatible with the necessity requirement[283]. With respect to the proportionality element, the Court required four safeguards in the government data access: (1) limited use of data for the purpose of national security, (2) not excessive retention of data (3) not merely using this data for the legal consequences (criminal conviction) and (4) effective judicial redress mechanism[284]. The Court decided that these safeguards are respected in the specific case and find the interference with the right to data protection and right to confidentiality of the communication compatible with the Constitution[285].

Personal data access by the General Directorate of Security and Gendarmerie of General Command

Tasks and competences of the General Directorate of Security and Gendarmerie of General Command

There are two powers of the Directorate and Gendarmerie related to personal data processing: access to information and documents held by public entities[286] and access to metadata and content of communication as well as signal detection[287].

Substantial and procedural conditions and safeguards for personal data access

Regarding information access, in contrast to the MIT's power, the Directorate and Gendarmerie can only request information and documents from public entities. Thus, the Directorate and Gendarmerie cannot request information from private entities. The general safeguards are similar to the general safeguards mentioned for the MIT's access to information and documents. In contrast to the powers of the MIT, the request has to be in writing and the Directorate has to justify its request. In addition, the Directorate shall get judicial approval if the public entities refuse to provide information based on incompatibility with the law in general, as well as trade secret reasons. Concerning access to telecommunication data as well as the content of communication, the safeguards converge with the safeguards for the MIT's power of access to telecommunication data. In contrast to the MIT's competences, there is no difference between foreigners and citizens in terms of safeguards. They have the same safeguards. The only difference with the conditions mentioned in the section for the MIT is that in case of urgency, judicial approval shall be taken within 48 hours rather than 24 hours.

2.2.2.2 OVERSIGHT MECHANISM FOR NATIONAL SECURITY ACCESS

The data processing activities by the intelligence organisations are not subject to the oversight of the Turkish SA due to Article 28 TPDPL. However, there are three *ex-post* external oversight mechanisms, which are relevant for intelligence activities. These oversight mechanisms apply to all intelligence activities unless it is stated otherwise.

The first is the administrative oversight by the State Supervisory Council, known as "*Devlet Denetleme Kurulu*" (DDK)[288]. The Council is a constitutional institution established within the Presidency, which

[282] [redacted]
[283] *Bestami Eroğlu* [GK], B. no: 2018/23077, T. 17/9/2020, paragraph 148, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/23077?BasvuruAdi=BESTAM%C4%B0+ERO%C4%9ELU.
[284] Ibid, paragraph 153.
[285] Ibid, paragraph 158.
[286] Add. Article 7(6) of Police Law and Add. Article 5(5) of Gendarmerie Law.
[287] Add. Article 7(2) of Police Law and Add. Article 5(1) of Gendarmerie Law.
[288] Article 6(8) of MIT Law; add. Article 7(9) of Police Law and Article 5(8) of Gendarmerie Law.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

is responsible for the oversight of public entities except for judicial bodies and has the power of investigation, examinations and inspections according to Article 108 of the Constitution. The president and members of the Council are appointed by the President[289]. Its powers are further specified in the Presidential Decree on the State Supervisory Council[290]. While the Council itself does not have corrective powers, based on its investigations and inspections, the Council can prepare reports and inform the prosecutors or relevant public entities to initiate judicial procedures if any irregularities are found[291]. This oversight mechanism is not open to public scrutiny.

The second *ex-post* external oversight mechanism is parliamentary oversight. The Security and Intelligence Committee has been established within the Grand National Assembly of Türkiye [292]. Annual reports have to be prepared by the MIT, the Directorate and the Gendarmerie, and are sent to the Presidency[293]. The annual report shall be submitted to the Security and Intelligence Committee each year. The Committee consists of 17 members according to the representation of political parties in the National Assembly[294]. The report that is provided to the Committee and the deliberations within the Committee are confidential[295]. One of the tasks of the Committee is to provide recommendations to protect the security of personal data obtained during security and intelligence services and the rights and freedoms of individuals. The EU progress report on Türkiye states that the oversight of security and intelligence organisations by the parliament must be strengthened considering the limited accountability of the police and security organisations[296]. The activities of the Committee are considered as confidential and not open to public scrutiny.

The third oversight mechanism is oversight by the Ombudsman, which was established in 2012 as a constitutional public entity affiliated with the Grand National Assembly of Türkiye[297]. It is an independent and impartial institution, which is tasked with investigating administrative practices and making recommendations to the administration in terms of compliance with the law in particular human rights' standards[298] based upon a complaint mechanism. Everyone has a right to file a complaint against the administrative act or decision according to Article 74(4) of the Constitution. The right to a complaint is granted to everyone, therefore, foreigners can also initiate a complaint against administrative acts or decisions if foreigners are affected by said decision or act.

The oversight by the Ombudsman is not specifically designed for government access to personal data for intelligence purposes. However, its scope is broad enough to extend to such data access according to Article 5 of the Law on the Ombudsman Institution numbered 6328 and dated 2012. As the right to data protection as well as the right to privacy are human rights recognised in the Turkish Constitution, the Ombudsman has the power of access to information and documents and of proposing non-binding recommendations to public entities, if they infringe the right to data protection or other fundamental rights. If the concerned public entity does not comply with the recommendation, it has to justify its non-compliance. For example, the Ombudsman issued a recommendation on the processing and storing of

[289] See for a criticism against the independence of the Council with respect to anti-corruption matters, EU Progress Report, 2022, p. 28.
[290] Presidential Decree on Devlet Denetleme Kurulu numbered 5 dated 15/07/2018, available at: https://www.mevzuat.gov.tr/MevzuatMetin/19.5.5.pdf.
[291] Ibid, Article 20.
[292] Additional Article 2(1) of the MIT Law. See for the critical analysis of the oversight regime: Olgunsoy, F. (2019), *The Impact Of Intelligence Activities In Fight Against Terror On Liberties: Turkey, United Kingdom, United States Of America* (PhD Thesis in Turkish), available at: http://nek.istanbul.edu.tr:4444/ekos/TEZ/60634.pdf.
[293] Add. Article 2(1) of MIT Law; Add. Article 7(9) of Police Law and Article 5(8) of Gendarmerie Law.
[294] Add. Article 2(3) of MIT Law.
[295] Add. Article 2(6) of MIT Law, see the suggestion of the publication of the report, Olgunsoy, F. (2019), *The Impact Of Intelligence Activities In Fight Against Terror On Liberties: Turkey, United Kingdom, United States Of America*(PhD Thesis in Turkish), available at: http://nek.istanbul.edu.tr:4444/ekos/TEZ/60634.pdf.
[296] EU Commission, *Türkiye 2022 Report*, pp. 5 and 17, available at: https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrkiye%20Report%202022.pdf.
[297] Article 74 of the Constitution.
[298] See the analysis of the Institution and its impact on fundamental rights, Alyanak, S., *The New Institution on Protection of Fundamental Rights: Turkish Ombudsman Institution*, available at: https://dspace.ankara.edu.tr/xmlui/handle/20.500.12575/42699.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

personal data of sensitive nature (criminal records) in the law enforcement database by the General Directorate of Security[299].

The Ombudsman received certain criticisms in the EU Progress Reports. The first one is that it does not have ex-officio investigation power and cannot issue legally binding decisions against public entities[300]. The second criticism is its silence on critical fundamental rights concerns[301]. Therefore, its oversight over the governmental data access might be considered limited.

2.2.2.3 JUDICIAL REDRESS MECHANISMS FOR NATIONAL SECURITY ACCESS: ADMINISTRATIVE, CRIMINAL AND CONSTITUTIONAL LAW REMEDIES

Individuals can exercise judicial redress mechanisms in administrative and constitutional law. As a requirement of the rule of law, an administrative action, which refers to any decision or action taken by an administrative authority in the exercise of its official powers, shall be subject to judicial review. Article 125 of the Constitution stipulates that judicial remedy is open against all kinds of acts of public entities. The acts of public entities are subject to the jurisdiction of the administrative and tax courts. Judicial review of the legality of the acts of the administration is ensured through annulment action and full compensation action.

An annulment action is a judicial process that checks whether the administrative action is unlawful. According to Article 2(1)(a) of Administrative Procedure Law of Türkiye[302], everyone including foreigners can initiate the annulment action if they meet the following conditions: (i) violation of interest, (ii) the existence of final and executable action, and (iii) exercise of the action within sixty days. For government data access, the annulment action can be used as long as these three conditions are met. The violation of data protection rights can be considered a violation of interest since data protection is considered a fundamental right under Article 20 of the Constitution. Data access by intelligence organisations is less likely to meet the second condition unless the processing of personal data leads the public entities to initiate a final and executable action against a natural person[303]. For instance, if the residence permit application of a foreign individual is denied based on personal data processing for intelligence purposes, the foreign individual can seek the annulment of a decision on the residence permit application. In this example, the reasoned decision of the administrative authority might refer to national security as a reason for the denial of the residence permit. If the foreign individual can seek the annulment of the decision on the residence permit application, during the proceedings, the Administrative Court can request the relevant information and review the legality of the decision and take into account the right to data protection as it is recognised as a fundamental right under Article 20 of the Constitution.

Individuals may also seek monetary compensation if administrative actions caused harm to individuals according to the Constitution[304]. For instance, in the individual complaint of *Yasemin Çongar and others*,

[299] Application no. 2019 4234, 23 August 2019, available at: https://kararlar.ombudsman.gov.tr/Arama/Download?url=20190219\19438\Yayin\Karar-2019-4234.pdf&tarih=2019-08-23T14:09:55.848612.
[300] EU Commission, *Türkiye 2022 Report*, p. 14.
[301] Ibid.
[302] The Administrative Procedure Law of Türkiye, numbered 2577, available at: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.2577.pdf.
[303] See for different decisions of the Administrative Court regarding the annulment actions in the case of personal data processing, Akman, N. G. (2021), *Protection of Personal Data by Administrative Law (Master Thesis)*, available at: https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=v7BkNnnepTnbhn8rNR77LcR_II-f_TK_3XoNmW2wSHu86pEYn4zgNqFITXoQxtnR.
[304] Article 125 of the Constitution.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

the Constitutional Court reward non-pecuniary damages to the complainants[305]. These non-pecuniary damages were awarded due to the violation of the right to the confidentiality of communications of the complainants. The violation occurred because while the MIT requested the judge to listen to the complainants' communications, the MIT did not write their real identities in the written request but wrote down a false identity to ensure the confidentiality of the investigations, which is against Article 6(4) of the MIT Law, which prescribes the indication of real names. The administration's non-contractual liability manifests itself in the form of faulty or strict liability. The procedure and conditions of seeking damages in administrative courts are regulated in the Administrative Procedure Law of Türkiye[306]. Regarding government data access, if the data is used for purposes other than those specified in the law, disclosed to third parties, and not deleted after the statute of limitations specified in the law, and as a result, the persons are exposed to material or moral harm, the administrative courts can require the state to pay damages to the individuals[307].

According to Article 148(3) of the Constitution, everyone who enjoys the rights and freedoms guaranteed by the Constitution may file a complaint with the Constitutional Court alleging that any of their freedoms protected by the ECHR have been violated by the state. Before applying, it is required that all possible legal remedies have been exhausted. As personal data protection and the right to privacy are considered fundamental rights, individuals can seek monetary or non-monetary damages in case of a violation of their right to data protection. In addition, the Court can order a retrial if it is necessary. In terms of government data access, the processing of personal data by intelligence organisations may not be considered an action of a state with public force unless it has further consequences for individuals. This is because the processing of personal data by intelligence organisations is generally a preparatory action before state authorities take further action. Therefore, it is very rare for an individual applicant to use this individual complaint remedy against such actions of the intelligence agencies as an individual might not realise that an intelligence activity is being carried out against him or her.

However, it is not impossible, considering the following examples. For instance, in the complaint of *Ercan Kanar,* he claimed that the MIT unlawfully collected his personal information in an intelligence report and that this report contained information on his personal, private, and professional status, which was included in the criminal investigation. The complainant argued that the disclosure was against, among others, Article 20 of the Constitution (right to privacy and data protection). The Court held that a serious interference to the applicant's private life had occurred by making his personal information available via inserting the intelligence report into the case file[308]. The Court stated that in a democratic society, it was unacceptable to insert intelligence information that had not been requested in any way and had not been subject to review. It could not be justified as necessary in a democratic society, nor could it be justified as proportionate[309]. More importantly, individuals can complain when a decision or an action is taken against them and has a legal effect such as a denial of entry to Türkiye or the freezing of their assets. For example, if individuals initiate a request to exercise their right of access, as will be discussed further in section 2.2.4, then if this request is rejected by intelligence organisations, individuals can initiate the judicial redress mechanism mentioned in this section. If they are not satisfied with the decisions of the courts, they can invoke their right to personal data protection before the Constitutional Court. Therefore, individuals can complain about the violation of the right to data protection after they have exhausted all remedies in criminal courts or administrative courts as a last recourse[310]. After the

[305] AYM, *Yasemin Çongar ve diğerleri [GK], B. No: 2013/7054, 6/1/2015,* available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/7054.
[306] See Articles 12-13 of the Administrative Procedure Law of Türkiye.
[307] See examples of actions for damages against the state in general, Akman, N. G. (2021), *Protection of Personal Data by Administrative Law* (Master Thesis), available at: https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=v7BkNnnepTnbhn8rNR77LcR_II-f_TK_3XoNmW2wSHu86pEYn4zgNqFITXoQxtnR.
[308] AYM, *Ercan Kanar,* B. No: 2013/533, 9/1/2014, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/533.
[309] Ibid, paragraph 61.
[310] See for the analysis of potential victim in case of intelligence activities, Olgunsoy, F. (2019), *The Impact of Intelligence Activities In Fight Against Terror On Liberties: Turkey, United Kingdom, United States Of America* (PhD Thesis), pp. 181-182, available at: http://nek.istanbul.edu.tr:4444/ekos/TEZ/60634.pdf.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

individual complaint mechanism, as Türkiye is a party to ECHR, it is also possible to initiate a complaint against Türkiye before the ECtHR.

2.2.2.4 GOVERNMENTAL ACCESS TO PERSONAL DATA FOR THE PURPOSE OF CRIMINAL INVESTIGATION AND PROSECUTION

Under Turkish Criminal Procedure Law (TCPL)[311], various tools are available for prosecutors and courts to gather evidence during a criminal investigation or prosecution. In general, these measures are carried out by law enforcement agencies under the supervision of prosecutors or courts. The judge of the criminal court of peace, which is the court at the location of the prosecutor who has made the request at the investigation stage, is authorised to decide on the measures, and the court hearing the case is authorised during the prosecution stage.

Among others, prosecutors, judges or courts may request any information in writing during the investigation and prosecution of offences, pursuant to Article 332 TCPL. Furthermore, Article 161(2) TCPL obliges other public officials to provide the requested information and documents without delay upon the request made by the public prosecutor. In contrast to Article 332, Article 161(2) does not specify any formal requirements for the information request by the public prosecutor. As an important note, failure of public officials to respond to an information request or to provide information or documents may constitute a crime of misconduct under Article 257 TCL.

Two measures available to the public prosecutor stipulated under the TCPL are of relevance for this study: (i) search of computers, computer programs and transcripts, copying and provisional seizure[312]; and (ii) interception of correspondence through telecommunication[313]. Given the amount of personal data that may be accessed or processed through individuals' computers or communications via telecommunications, the remainder of this sub-section focuses on the conditions and safeguards provided by law for the application of these investigatory measures.

Search of computers, computer programs and transcripts, copying and provisional seizure

Article 134 TCPL allows for searching the computers, computer programs and computer logs used by a suspect, and for making copies of computer records and decoding and transcribing these records for the purpose of obtaining evidence during an ongoing investigation or prosecution. The provision provides additional safeguards for the suspects and accused such as during the seizure of computers or computer logs, all data in the system shall be backed up[314] and if requested by the suspect or his or her attorney, a copy of this backup shall be made and given to the suspect or his or her attorney, and this shall be recorded in a report and signed[315]. A copy of all or part of the data in the system may be taken without seizure of the computer or computer logs. The copied data shall be printed on paper and this matter shall be recorded in the minutes and signed by the relevant persons[316]. Following the amendment made to the provision in Article 16 of the Law No. 7145 dated 25 July 2018, additional safeguards and time limitations are introduced. In this vein, decisions issued by the public prosecutor shall be submitted for the approval of the judge within 24 hours. The judge shall render his or her decision within 24 hours at the latest. If the time limit expires or if the judge decides otherwise, the copies and transcripts shall be destroyed immediately[317].

[311] The Criminal Procedure Law of Türkiye, numbered 5271 and dated 2004, available at: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5271.pdf.
[312] Article 134 TCPL.
[313] Article 135 TCPL.
[314] Article 134(3) TCPL.
[315] Article 134(4) TCPL.
[316] Article 134(5) TCPL.
[317] This amendment is introduced as a safeguard in line with the Article 20 of the Constitution.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Interception of correspondence through telecommunication

Pursuant to Article 135(1) TCPL, the telecommunication of a suspect or defendant may be intercepted, recorded and signal information may be evaluated[318] with the decision of the judge or, in case there is urgency by the public prosecutor, to obtain evidence in relation to an ongoing investigation or prosecution of certain crimes. The provision requires the existence of a strong suspicion that certain crimes listed in the law have been committed as a condition for the application of the measure. In line with ECtHR case law[319], this measure can only be applied if it is impossible or very difficult to establish material facts by other means in order to prevent arbitrary practices. The provision states that the measure can be applied for a maximum period of three months, and it is foreseen that this period can be extended at most once. With the amendment made to the Article 135(3) TCPL, the duration of the measure may be extended several times for a period not exceeding one month each time, but no upper limit is foreseen for organised crimes. This measure is applied in secret, and therefore, it is not possible for the person against whom the measure is applied to be aware of it.

Under the same provision, Article 135(6) TCPL regulates the detection of a suspect's or defendant's telecommunications, i.e. Historical Traffic Search (HTS), independently of the other measures provided for in Article 135(1) TCPL[320]. The application of Article 135(6) is subject to similar safeguards deriving from Article 20 Constitution, such as the requirement of a judge's decision or, in urgent cases, the decision of the public prosecutor, provided that it is submitted to the judge within 24 hours. However, Article 135(6) TCPL does not require the strong suspicion or limited applicability to certain offences as a precondition for the applicability of this measure, as provided for in Article 135(1) TCPL. Thus, the detection of the suspect's or defendant's telecommunications may find wider scope of the application in criminal investigations and prosecutions compared to the measures stipulated under Article 135(1) TCPL[321].

As an additional safeguard, Article 136 TCPL stipulates that the communication of the suspect or defendant with his or her defence counsel cannot be monitored and intercepted. According to Article 137(4) TCPL, when the data obtained via this measure are destroyed, the Public Prosecutor's Office must inform the relevant person in writing about the reason, scope, duration and result of the measure within 15 days at the latest from the end of the investigation phase. In cases where the data obtained used in the investigation and a lawsuit is filed against the relevant person, the relevant person is not notified separately about the measure because, the indictment is notified to the person concerned, and the person concerned has learnt that the measure has been applied. In case the measure is applied at the prosecution stage, it is not possible to apply the measure secretly.

The procedural and substantial conditions and safeguards

Given the intrusiveness of the aforementioned measures and their potential implications on the fundamental rights, the legislator regulated these two measures as a "last resort" to obtain the evidence. In other words, if it is possible to obtain evidence by other means, in principle, these measures cannot be applied except the detection of the communication as stipulated under Article 135(6) TCPL. In this regard, other conditions and limitations are introduced in the provisions such as "limited duration" of the measure, "transcribing records" and all the data obtained, and "if there are strong indications of suspicion that crime is attempted". These measures might be applied in case there is "strong

[318] The TCPL does not specify whether historical traffic search (HTS) records that were retained by telephone operators "prior to the date of the decision" can be requested or used in the ongoing investigation or prosecution of a crime.
[319] Judgment of the European Court of Human Rights of 6 September 1978, *Klass and ors v Federal Republic of Germany*, Judgment, Merits, no 5029/71 (A/28), (1979-80) 2 EHRR 214, IHRL 19 (ECHR 1978).
[320] Article 135(6) TCPL.
[321] Article 135(5) TCPL also regulates a specific measure for the determination of the location of suspects of defendants' mobile phone in order to catch them, based on the decision of the judge or in case there is urgency with the decision of the prosecutors, without the need for seeking judges' approval. This measure also can be applied maximum of three months.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

suspicion"[322] that one or more of the offences listed in the relevant provisions have been committed. It means that a simple suspicion is not sufficient for the application of these measures. In case, there is urgency, those measures can be initiated by the decision of the public prosecutor alone, with the condition that the rendered decision shall be submitted for the approval of the judge within 24 hours and the judge shall decide in 24 hours at the latest. Those measures expire in the event of a decision of non-prosecution or the termination of suspicion, the conclusion of the case, the disappearance of other conditions related to the measure, anytime with the decision of the prosecutor or in the event that the decisions made by the public prosecutor are not submitted for the approval of the judge within 24 hours or the cautionary decisions submitted for approval are not decided by the judge within 24 hours and are not approved by the judge. Based on the aforementioned conditions and safeguards, the Constitutional Court also found some of these measures proportionate, legitimate and compliant with the Constitution[323].

2.2.2.5 JUDICIAL REDRESS MECHANISMS IN CASE OF LAW ENFORCEMENT ACCESS TO PERSONAL DATA

The application of the measures explained in section 2.2.2.4 without a judge's decision or, in exceptional cases, a prosecutor's decision is unlawful, and hence the data obtained in this way can neither be used as evidence nor form the basis of a judgment[324]. Moreover, the Court of Cassation also takes into account the absence of the judge's decision regarding the surveillance of communication in the file, or not being submitted to the file, or not being read at the hearing, and taking the judgment without discussing the legality of the data obtained in a clear manner as sufficient grounds for reversal[325]. Moreover, misuse of these measures can amount to "Crimes against Private Life and Confidentiality of Life" as punished under the TCL and criminal liability of officers who take part in the application of the measure can be evoked.

The TCPL also allows defendants to challenge the decisions related to the measures rendered by the Court, judge or in certain cases by prosecutors within the period of seven days starting from the notification of the decision[326]. If there is any material or moral damages arising from one of the applied measure listed under Article 141 TCPL, individuals may claim all kinds of material and moral damages[327]. Another available judicial redress mechanism is the complaint mechanism described above for measures of public authorities that can be used by suspects or defendants who are subject to the one of the aforementioned measures to claim a violation of their rights guaranteed under the ECHR. In compliance with Turkish Law, the mentioned safeguards apply to all individuals, including foreigners, before the courts without any specific limitation.

2.2.3 DATA SUBJECT RIGHTS

The Turkish Constitution recognises that the right to data protection includes the following data subjects' rights: (i) right to be informed, (ii) right of access, (iii) right of rectification and deletion and (iv) right to know whether his or her data is processed in line with the specified purpose. The Constitutional Court

[322] Strong suspicion means that when there is a strong probability of conviction at the end of the judgement to be made according to the available evidence.
[323]See, AYM, E.2018/137, K.2022/86, 30/06/2022, paragraphs 346-368, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/86.
[324] This is also guaranteed by Article 38(6) of the Constitution: "*Findings obtained through illegal methods shall not be considered evidence.*"
[325] See also decision from the Court of Cassation Yargıtay Yargıtay Ceza Genel Kurulu, 17.02.2006, 2006/5 E, 2006/180 K; Yargıtay Ceza Genel Kurulu 04.07.2006, E. 2006/5-127, K. 2006/180; Yargıtay Ceza Genel Kurulu, 14.10.2008, E.2008/8-49, K. 2008/219.
[326] Article 268/3 CPL.
[327] See the broad interpretation of the Article 141 TCPL by the Court of Cassation; see AYM, İlhan Gökhan, B. No: 2017/27957, 9/9/2020, paragraphs 24-27, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2017/27957.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

referred to these rights while determining the scope of right to personal data protection in its case law[328]. The Court explicitly stated that the right to personal data in Article 20 of the Constitution included these data subject rights and any interference with these rights needed to respect the constitutional protection[329]. The importance of recognising these rights at the constitutional level is that if individuals are not satisfied with the data subject rights given to them in the secondary legislation or in practice, they can make an individual complaint before the Constitutional Court.

Despite the fact that these rights are recognised at the constitutional level, the exercise of these rights is to be further defined in secondary legislation, including by setting the conditions to use them. For instance, the TPDPL recognises these rights. However, individuals cannot exercise the data subject rights recognised under the TPDPL when personal data are processed either for intelligence, crime prevention or crime investigation and prosecution purposes. This is because the processing of personal data for intelligence activities, criminal investigation as well as prosecution are excluded from the TPDPL according to Article 28(1)(ç). Indeed, it can be argued that individuals can exercise the right of access and the right to be informed in relation to private entities in accordance with Article 11(ç) under the TPDPL for the government access for intelligence purposes. However, due to the sensitive nature of data access for intelligence purposes, private entities may not disclose the scope of access because doing so could result in the disclosure of intelligence information or operations in general, which could jeopardise intelligence activities carried out by intelligence organisations.

The right to obtain information in the Constitution can be considered as a way of exercising the right of access in the absence of data subject rights. This right is recognised in Article 74(4) of the Constitution as well as in the Law on the Right to Information, dated 2003 and numbered 4982[330]. Similarly, the Constitutional Court in a judgment of January 2023, considered this right of information as a data subject access right, which is recognised in Article 20 of the Constitution for individuals[331]. The Constitution recognises this right for everyone and Article 4(1) of the Law on Right to Information reiterates this. However, Article 4(2) states that only foreigners domiciled in Türkiye, subject to the principle of reciprocity, can exercise the right to information. Thus, it seems that this right cannot be exercised by foreigners residing outside of Türkiye if Article 4(2) is interpreted restrictively. However, as the Constitution recognises this right to everyone without any limitations, this type of interpretation can be considered incompatible with Article 74(4) of the Constitution. Therefore, it can be argued that foreigners residing outside Türkiye can also exercise this right.

While the right to obtain information from intelligence entities or judicial entities is limited, they are not fully excluded from its scope. For the information processed in the context of judicial investigations or prosecutions (Article 20), access requests will not be met if the disclosure prejudices the criminal investigation. It is not possible to initiate an access request for information or documents concerning state intelligence, unless they affect the professional honour and working life of the person according to Article 18(2) of the Law on Right to Information. As the professional honour and working life of the person is not defined in this law, the ordinary meaning of the term has to be considered relevant. In particular, if any intelligence provided by the MIT leads a public entity to not assign a person to a specific role within the state might affect the professional life of a person.

Access requests by individuals are further restricted by an additional paragraph added to Article 30 of the MIT Law[332]. According to Article 30(5) of the MIT Law, the MIT is fully excluded from the scope

[328] One of the interviewees refers to one of the latest cases in relation to the data subject rights, see AYM, *Ümit Eyüpoğlu*, B. No: 2018/6161, 28/6/2022, paragraph 18, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/6161.
[329] Ibid, paragraph 48.
[330] The purpose of the law according to Article 1 is to exercise the right of individuals to obtain information in accordance with the principles of equality, impartiality and openness, which are the requirements of democratic and transparent administration, available at: https://www mevzuat.gov.tr/mevzuatmetin/1.5.4982.pdf.
[331] AYM, E.2018/137, K.2022/86, 30/06/2022, paragraph 134, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2022-86-nrm.pdf.
[332] One of the interviewees mentions this new exclusion and refers to this new case, AYM, E.2018/137, K.2022/86, 30/06/2022, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/86.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

of Law on the Right to Information. However, the Constitutional Court, in its decision numbered 2022/86, which was published on 12 January 2023, found this additional paragraph (Article 30(5) of the MIT Law) incompatible with Article 20 (right to data protection) and Article 74 (right to obtain information) of the Constitution[333]. In its reasoning, the Court stated that it is possible that some of the information and documents to which the rule prohibits access are personal data. The Court stated that excluding the possibility of accessing documents and information related to his/her social life by individuals prevent its correction and deletion, thus, it constitutes an interference with the right to personal data[334]. The Court underlined the importance of access to personal data for preventing arbitrary practices in the democratic and transparent exercise of public power[335]. While the Court found that the interference is restricted by law and pursues a legitimate interest, the complete exclusion of MIT from the scope of right of access cannot be considered as proportionate[336]. The Constitutional Court stated that personal data access is possible within the defined scope under the Law on Right to Information. Therefore, individuals may exercise the right to obtain information about their personal data processing as long as the information affects their professional honour and working life.

There is no possibility for individuals to obtain confirmation of the legality of data processing by an administrative independent authority. However, if the access to information request is not fulfilled at all or individuals consider that the information processed is illegally obtained, the response to the request can be considered as an administrative action, and they can initiate the annulment action, which has been discussed above in section 2.2.2.1, regarding the decision by the MIT before the administrative courts.

Moreover, in the context of criminal investigations and prosecutions, within the framework of Article 153 TCPL, the defence counsel of the suspect has the right to examine the case file and can access the information gathered through these measures. This can be considered as a way of exercising a right of access.

2.2.4 OVERVIEW OF RELEVANT LEGISLATION

Public authority activity	Laws applied	Oversight	Redress mechanisms
National Security	MIT Law	Parliament Oversight Ombudsman State Council Ex-ante judiciary review for certain measures (access to metadata and content data for the citizens living inside Türkiye)	Judiciary
National Security, Crime Prevention	Police Law Gendarmarie Law	Parliament Oversight Ombudsman State Council Ex-ante judiciary review for accessing to the metadata and content data of communications	Judiciary
Crime Investigation and Prosecution	TCPL	Ex-ante judiciary review for the computer seizure and	Judiciary

[333] Ibid, paragraph 188.
[334] Ibid, paragraph 174.
[335] Ibid, paragraph 188.
[336] Ibid.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

		interception of correspondence through telecommunication	

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

3 CONCLUSION

This study has assessed the relevant legal frameworks and practices around governmental access for the countries of Mexico and Türkiye. The paragraphs below summarise the main findings of the report for each of the assessed jurisdiction.

Mexico has a robust legal system for data protection, with the constitutional text protecting not only the right to data protection but also the ARCO rights (access, rectification, cancelation, and objection). This guarantees that data protection rights are applied to any person, regardless of their nationality, having access to the whole National Transparency System. The protection of personal data is mainly ensured by two general laws: one focused on the private sector (LGPDSSP) and one on the public sector (LGPDSSO). Both laws serve as a general parameter that must be implemented in all the different jurisdictions of the Mexican federation. Thus, the decentralised system leads to the existence of different data protection authorities, also responsible for overseeing the transparency rules. The INAI has a crucial role in overseeing the regional authorities while working side by side with federal authorities. The INAI competences also complement the role of judicial authorities in overseeing surveillance measures.

Governmental access for the purpose of national security is outside the scope of these general data protection laws. These activities should observe the National Security Law (NSL), which also foresees different mechanisms to guarantee the principle of data minimisation and information security. However, data processing for national security reasons lacks any details on the oversight of these activities. Considering that national security is an exception for the data protection laws, there is uncertainty on the extent to which the competent data protection authorities can act on these matters. The main challenges therefore seem to be related to the establishment of a structured oversight system. Reported difficulties also include the guaranteeing of a harmonised application of the different levels of norms, ensuring the independence of the existing authorities, and resisting political interference with such authorities. Upcoming legal initiatives should not undermine the already existing safeguards and rights, but further a proportional approach to develop security and privacy.

Türkiye has a strong constitutional protection for personal data protection. Article 20 of the Turkish Constitution explicitly recognises personal data protection as a fundamental right in addition to right to privacy. This right is granted to everyone including foreigners and includes a right to be informed, a right of access, a right to rectification, and a right to be forgotten. Despite the broad protection given at the constitutional level, the TPDPL, which ensures personal data protection at the secondary level, excludes the processing of personal data by judicial authorities, law enforcement and intelligence organisations. This exclusion of the data processing activities by intelligence and law enforcement authorities from the TPDPL does not mean that these organisations can process personal data arbitrarily. Considering the respective safeguards and oversight mechanisms, the Constitutional Court stated that the exclusion of the data processing activities by these organisations from the TPDPL is necessary and proportionate. Moreover, as confirmed during interviews, several amendments to the TPDPL are expected to be introduced in 2023 in order to align with the GDPR rules, although the details of the amendments are not yet clear or accessible. Individuals regardless of whether they are residing in Türkiye can seek ex-post judicial redress. Furthermore, they can initiate individual complaints of violation of the right to privacy and the right to data protection before the Turkish Constitutional Court after exhausting possible legal remedies. If individuals are not satisfied with the decision of the Constitutional Court, they can claim a violation of their rights guaranteed under the ECHR before the ECtHR.

Yet, the proportionality of government data access is questionable in four regards. First, the substantial and procedural conditions for the government data access for intelligence purposes, lack reference to the requirements of proportionality and necessity of the measure. Second, as it is raised in the dissenting opinion of the Constitutional Court in the case on the MIT Law, lowering safeguards for citizens living abroad and foreigners might not be justified without imposing further substantial and procedural

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

conditions, which substantiates the notion of necessity and proportionality. Third, despite the fact that three ex-post judicial redress mechanisms are available, other oversight mechanisms (parliamentary oversight, DDK`s oversight and Ombudsman's oversight) are limited since they are not specifically designed for an independent oversight of data processing activities for these purposes. Fourth, despite the recognition of the data subject rights at the constitutional level, the rights are not further recognised in the legislation except for a limited right to information and a right of access. However, this does not prevent individuals from invoking the constitutional data subject rights. If public entities do not respond to these rights' requests or individuals are not satisfied with the responses, individuals can invoke these rights before the Constitutional Court after exhausting legal remedies.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

ANNEX 1 – QUESTIONNAIRES

Mexico

General questions

1. Both the Law on the Protection of Personal Data in the Possession of Private Parties (LFPDPPP) and the Law on the Protection of Personal Data in possession of Public Parties (LGPDPPSO) foresee different rights for the data subjects. Are data subjects finding more difficulties in exercising their rights in one of the systems when compared to the other?

2. Do the provisions in data protection law (specially the LGPDPPSO) that foresee that every person has the right to data protection guarantees mean that foreigners, including EU citizens, residing inside or outside of Mexico can exercise their rights to guarantee the protection of their personal data?

3. Touristic areas have adopted various surveillance technologies because of the rise of security concerns. In this matter, the National Commission of Human Rights has published a recommendation highlighting the lack of regulation of the use of these technologies. Are there any existing bills about the regulation on how surveillance technologies should or can be used by public authorities in public spaces? What are the current policies and legal developments in this area?

4. Considering the Mexican open data initiative, is there any evidence of inaccuracy or negative effects regarding the information published/made available?

5. What are the legal safeguards regarding data sharing between public authorities also considering the open data initiative adopted in Mexico and the Law on the Protection of Personal Data in the possession of Public Parties (LGPDPPSO)? What are the main risks foreseen for public initiatives that rely on data sharing between public authorities (e.g., national ID card scheme)?
6. Are there any restrictions on data subjects' rights when the purpose of the processing of data is intelligence or national security?

7. Are there any ongoing legislative or policy developments that address the use of technology by third countries such as the US that directly affect data subjects in Mexico (e.g., use of facial recognition by the US government in the borders with Mexico)?

8. What are the regulations on data sharing from one Mexican public authority to another (onward sharing)? How do the data subject rights apply in these situations?

9. What are the existing rules regarding data transfers from Mexico to other (third) countries, especially when the personal data was collected or accessed by a Mexican public authority?

Data subject rights and legal remedies

10. What are the enforcement powers of INAI (Federal Institute for Access to Public Information and Data Protection) when it comes to criminal procedures or national security law? How do these provisions apply in cases of interception of private communications?

11. What is INAI's role in overseeing regional activities regarding the processing of data by local public authorities? Does this also apply to the evaluation of Data Protection Impact

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Assessments (*Evaluaciones de Impacto en la Protección de Datos Personales*)? Do public authorities have to prove the security of the systems used by them in data processing activities?

12. What mechanisms does INAI have to report infringements of the law to judicial courts (Article 89 of the LGPDPPSO)?

13. Are the guidelines and recommendations published by INAI used by judicial courts in decisions regarding data protection?

14. The General Law for Transparency obliges authorities involved in communication surveillance to publish periodic reports, including the judicial authorisations that led to the surveillance measure (e.g., Article 18). However, the telecommunications' regulators removed the transparency obligations foreseen in the previous Guidelines for Collaboration on Security and Justice Matters. How is this system currently working? Are there any obligations regarding this topic?

15. Does the legal system determine when the data subject should be notified after she/he was targeted with a surveillance mechanism (e.g., intercept of private communications)? Are there any legal provisions on how and when the unnecessary data should be deleted?

16. Article 68, III, of the General Law for Transparency, foresees the obligation of informing data subjects about aspects of the processing of personal data, but this obligation does not apply when the public authorities are acting within their legal attributions. In this scenario, how does the principle of transparency apply?

17. Considering the recent decisions of the Supreme Court of Justice, what are the existing mechanisms to modify a decision published by INAI?

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Türkiye

General Questions

1. What is your opinion on government data access in Türkiye and existing data protection safeguards for data subjects? (Please consider the broad exceptions for data processing for law enforcement and intelligence purposes in Türkiye.)

2. How is personal data protected while there's no specific law about processing for criminal prosecution, national defence and security or public safety?

3. What are the legal protection mechanisms provided to foreigners, including EU citizens, residing outside Türkiye in case of processing their data for law enforcement purposes as well as intelligence purposes? (Please consider legal remedies such as at courts, complaint mechanisms at the authorities themselves, or at a supervisory authority.)

4. Do foreigners, including EU Citizens, have equivalent protection of their fundamental rights when their personal data are processed for law enforcement purposes and in case of government access to data? (Please compare with data subjects residing in Türkiye.)

5. What are the legal rules on data transfers from Türkiye to other countries, especially for governmental authorities who might have previously received that data via governmental access?

Data Subject Rights and Legal Remedies

6. Do data subjects have any rights and safeguards (e.g., legal remedies to invoke at court or a public authority to gain access, rectification or erasure) when their personal data are processed for law enforcement and intelligence purposes? If so, what are the limitations? (e.g., considering the data protection law, criminal procedural law, right to information, constitutional law etc.)

7. What do you think about the feasibility of invoking the right to information (e.g., Presidency's Communication Centre etc.) as a data access right in case of processing personal data by law enforcement and intelligence services?

8. As a follow-up to question 5, what do you think about the available rights and safeguards in case of unlawful processing of personal data by law enforcement authorities or intelligence services (i.e., administrative law, criminal law, constitutional law)?

9. As a follow-up to question 5, are there any limits to these rights and safeguards specific to the case of a foreign data subject, including EU citizens, who wants to rely on them, residing outside Türkiye?

Possible objection mechanisms to government access request

10. If a government access request is made to economic operators (e.g., Internet service providers, telecommunication providers) in Türkiye, what are the processes that need to be carried out to fulfil this request? (Please answer the question considering the different applicable regimes to requests by law enforcement and intelligence agencies.)

11. Are there any legal objection mechanisms provided to economic operators against the request made by the requesting government authorities?
    a. If the answer is yes to question 11, how does it occur in practice?

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

b. If the answer is no to question 11, is there any possibility of informing data subjects about government data access?

Upcoming legal initiatives

12. Are there any upcoming policy or legal initiatives concerning data protection and government access to personal data in Türkiye? (Please consider the scope and adequacy of the proposed amendments to the data protection law.)

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

ANNEX 2 – SOURCES OF INFORMATION

General Part

Case law

CJEU

Judgment of the Court (Grand Chamber) of 20 September 2022, C-339/20 VD and C-397/20 SR, ECLI:EU:C:2022:703.

Judgment of the Court (Grand Chamber) of 5 April 2022, *G.D v The Commissioner of the Garda Síochána, and Others*, C-140/20, ECLI:EU:C:2022:258.

Judgment of the Court (Tenth Chamber) of 21 October 2021, *the Spetsializiran nakazatelen sad*, C-350/21, ECLI:EU:C:2021:874.

Judgment of the Court (Eighth Chamber) of 2 September 2021, *Telekom Deutschland GmbH v Bundesrepublik Deutschland*, C-794/19.

Judgment of the Court (Grand Chamber) of 22 June 2021, *Ordre des barreaux francophones et germanophone and others*, C-512/18, ECLI:EU:C:2021:505.

Judgment of the Court (Grand Chamber) of 2 March 2021, *Prokuratuur*, C-746/18, ECLI:EU:C:2021:152.

Judgment of the Court (Grand Chamber) of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790.

Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18, ECLI:EU:C:2020:791.

Judgment of the Court (Grand Chamber) of 16 July 2020, *Schrems II*, C-311/18, ECLI:EU:C:2020:559.

Judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige*, C-203/15 and C-698/15, ECLI:EU:C:2016:970.

Judgment of the Court (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14 ECLI:EU:C:2015:650.

Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.

Judgment of the Court (Fourth Chamber) of 17 October 2013, *Michael Schwarz v. Stadt Bochum*, C-291/12, ECLI:EU:C:2013:670.

Judgment of the Court (Grand Chamber), 26 February 2013, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2013:107.

Judgment of the Court (Grand Chamber) of 16 December 2008, *Satakunnan and Satamedia Oy*, C-73/07, ECLI:EU:C:2008:727.

Judgment of the Court of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596.

Judgment of the Court (Grand Chamber) of 20 September 2022, *Bundesrepublik Deutschland v SpaceNet AG and Telekom Deutschland GmbH.SpaceNet*, C-793/19, ECLI:EU:C:2022:702.

ECtHR

Judgement of 25 May 2021, *Big Brother Watch and Others/The United Kingdom*, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013.

Judgement of 4 December 2015, *Zakharov v. Russia*, no. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306.

Judgement of 18 May 2010, *Kennedy v. the United Kingdom*, no. 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905.

Judgement of 2 December 2008, *K.U. v. Finland*, no. 2872/02, ECLI:CE:ECHR:2008:1202JUD000287202.

Judgement of 29 June 2006, *Weber and Saravia*, no. 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Judgement of 4 March 2004, *M.C. v. Bulgaria*, no. 39272/98, ECLI:CE:ECHR:2003:1204JUD003927298.
Judgement of 4 May 2000, *Rotaru v Romania*, no. 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195.
Judgement of 16 February 2000, *Amann v. Switzerland*, no. 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895.
Judgement of 28 October 1998, *Osman v. United Kingdom*, no. 23452/94, ECLI:CE:ECHR:1998:1028JUD002345294.
Judgement of 24 April 1990, *Huvig v. France*, no. 11105/84.
Judgement of 26 March 1987, *Leanderv. Sweden*, no. 9248/81, ECLI:CE:ECHR:1987:0326JUD000924881.
Judgement of 2 August 1984, *Malone v. the UK*, no. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179.
Judgement of 26 April 1979, *The Sunday Times v. the UK*, no. 6538/74, ECLI:CE:ECHR:1979:0426JUD000653874.

Opinions

Opinion of the Court (Grand Chamber) of 26 July 2017, Opinion 1/15 on the EU-Canada PNR Agreement, ECLI:EU:C:2017:592.

Other sources

European Data Protection Board (2023), *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*, Version 2.0.
European Data Protection Board (2020), *Guidelines 10/2020 on restrictions under Article 23 GDPR*.
European Data Protection Board (2020), *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*.
European Data Protection Supervisor (2017), *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a Toolkit*.
European Data Protection Supervisor (2021), *Case Law Digest: Transfers of personal data to third countries*.
European Data Protection Supervisor (2019), *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*.
European Union Agency for Fundamental Rights and the Council of Europe, *Handbook on European data protection law*, Publications Office of the European Union, Luxembourg, 2018.
Gerards, J., 'How to improve the necessity test of the European Court of Human Rights', *International Journal of Constitutional Law*, Vol. 11, No 2, April 2013, pp. 466–490.
Lenaerts, K., 'Limits on Limitations: The Essence of Fundamental Rights in the EU', *German Law Journal*, Vol. 20, pp. 779-793, Cambridge University Press, 2019.
Brkan, M., 'The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning', *German Law Journal*, Vol. 20, pp. 864-883, Cambridge University Press, 2019.
Tridimas, T., Gentile, G., 'The essence of Rights: An Unreliable Boundary?', *German Law Journal*, Vol. 20, pp. 794–816, Cambridge University Press, 2019.
Tracol, X., 'Ministerio fiscal: Access of public authorities to personal data retained by providers of electronic communications services', *European Data Protection Law Review*, Vol. 5, No 1, pp. 127-135.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Mexico

Case law

Supreme Court of Justice (*Suprema Corte de Justicia*), *Amparo Directo en Revisón* 6489/2018.

Supreme Court of Justice (*Suprema Corte de Justicia*), Case n. 2005522, Thesis P. II/2014, January 21st of 2014.

Supreme Court of Justice (*Suprema Corte de Justicia*), Case n. 2011608, Thesis 2a. XIX/2016 (10a), May 2016.

Supreme Court of Justice (*Suprema Corte de Justicia*), Case n. 2018460, Thesis I.10o.A.70 A (10a), November 2018.

Supreme Court of Justice (*Suprema Corte de Justicia*), Case n. 2024641, Thesis 2a./J. 23.2022 (11a), May 2022

Supreme Court of Justice (*Suprema Corte de Justicia*), *Controversia Constitucional*, P.J. 136/2005.

Legislation

Congreso General de los Estados Unidos Mexicanos, Código Nacional de Procedimientos Penales, March 2014, available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf.

Congreso General de los Estados Unidos Mexicanos, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, July 2010, Spanish text available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

Congreso General de los Estados Unidos Mexicanos, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, January 2017, Spanish text available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.

Congreso General de los Estados Unidos Mexicanos. Ley General de Transparencia y Acceso a la Información Pública, May 2015, Spanish text available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP_200521.pdf.

Congreso de los Estados Unidos Mexicanos, Ley de Seguridad Nacional, January 2005, Spanish text available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf.

Mexico, Constitución Política de los Estados Unidos Mexicanos, 1917, English version available at: https://www.constituteproject.org/constitution/Mexico_2015.pdf?lang=en.

Other sources

Article 19 (2022), *Mexico: Article 19 condemns continued assault on its work and the press*, Press release, available at: https://www.article19.org/wp-content/uploads/2022/12/article19_2022_comunicado_ingles.pdf.

CNI, *Aviso de Privacidad Integral*, available at: http://www.cni.gob.mx/transparencia/docs/Aviso-Privacidad-Integral.pdf.

CNI, *Guía para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales*, available at: http://www.cni.gob.mx/transparencia/docs/Guia-ARCO.pdf.

Estado de México, Periódico Oficial Gaceta del Gobierno y LEGISTEL, Leyes Nacionales, Generales y Federales, available at: https://legislacion.edomex.gob.mx/leyes_federales.

Estrada, J. M. M. (2015), *Configuración normativa de las leyes en el marco competencial de los órdenes jurídicos, Congreso Redipal Virtual VIII*, available at: https://www.diputados.gob.mx/sedia/sia/redipal/CRV-VIII-14-%2015.pdf.

García, A. G. (2016), *Transparency in Mexico: An Overview of Access to Information Regulations and their Effectiveness at the Federal and State Level*, Report, Wilson Center Mexico Institute.

Human Rights Watch (2019), *México: La transparencia y la privacidad, amenazadas*, available at: https://www.hrw.org/es/news/2021/01/28/mexico-la-transparencia-y-la-privacidad-amenazadas.

INAI, *El ABC del aviso de privacidad. Sector Público*, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_ABC-AP-SPublico.pdf.

INAI, *Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/_GuiaPrincipiosDeberes.pdf.

INAI (2022), *Informe de Labores 2022*, available at: https://micrositios.inai.org.mx/informesinai/.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

INAI (2022), *Recomendaciones para los sujetos obligados en las comunicaciones de datos personales*, available at: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones-SO_Comun_DP.pdf.

Lopes, T. M. G., 'Las recientes reformas em materia de protección de datos personales em México', *Anuario Jurídico y Económico Escurialense*, XLIV, 2011, pp. 317-334, ISSN: 1133-3677.

López, L. C. J., 'Seguridad nactional, inteligencia militar y acceso a la información en México', *URVIO Revista Latinoamericana de Estudios de Seguridad*, No 21, 2017, available at: http://scielo.senescyt.gob.ec/scielo.php?pid=S1390-42992017000100140&script=sci_arttext.

López, S. T., 'Sustitución de la Ley Federal de Archivos de México: el alcance de una ley general', *Revista Española de la Transparencia*, No 12, January - June 2021, pp. 167-187.

Mexico, Senado de la República, Código Nacional de Procedimientos Penales, 2014, available at: senado.gob.mx/comisiones/justicia/docs/CNPP.pdf

Mexico, Lineamientos Generales de Protección de Datos Personales para el Sector Público, 2017, available at: https://www.gob.mx/cms/uploads/attachment/file/304930/lineamientos_generales_para_la_protecci_n_de_datos_personales_para_el_sector_p_blico.pdf.

OECD (2022), *Declaration on Government Access to Personal Data Held by Private Sector Entities*, available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Türkiye

Case Law

Judgment of the European Court of Human Rights 6 September 1978, *Klass and ors v Federal Republic of Germany*, no. 5029/71 (A/28), (1979-80) 2 EHRR 214, IHRL 19 (ECHR 1978).

AYM, *Bestami Eroğlu [GK]*, B. No: 2018/23077, T. 17/9/2020, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/23077?BasvuruAdi=BESTAM%C4%B0+ERO%C4%9ELU.

AYM, E.2019/96, K.2022/17, T. 24/02/2022, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/17.

AYM, E.2018/137, K.2022/86, 30/06/2022, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2022/86.

AYM E.2016/125., K.2017/143, 28/09/2017, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2017/143?KararNo=2017%2F143.

AYM, E.2014/122, K.2015/123 T. 30/12/2015, available at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2015/123.

AYM, *Ercan Kanar*, B. No: 2013/533, 9/1/2014 available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/533.

AYM, *İlhan Gökhan*, B. No: 2017/27957, 9/9/2020, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2017/27957.

AYM, *Ümit Eyüpoğlu*, B. No: 2018/6161, 28/6/2022, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/6161.

AYM, *Yasemin Çongar ve diğerleri [GK]*, B. No: 2013/7054, 6/1/2015, available at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/7054.

The Ombdusman Institution, Application No. 2019 4234, 23 August 2019, available at: https://kararlar.ombudsman.gov.tr/Arama/Download?url=20190219\19438\Yayin\Karar-2019-4234.pdf&tarih=2019-08-23T14:09:55.848612.

Legislation

The Administrative Procedure Law of Türkiye, numbered 2577 and dated 1982, available at: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.2577.pdfhttps://www.mevzuat.gov.tr/mevzuatmetin/1.5.2577.pdf.

The Constitution of the Republic of Türkiye provided by Grand National Assembly of Türkiye, GNAT, May 2019, available at: https://www5.tbmm.gov.tr/yayinlar/2021/TC_Anayasasi_ve_TBMM_Ic_Tuzugu_Ingilizce.pdf.

The Law on the Duties and Powers of the Gendarmerie Organization, dated 1983 and numbered 2803 (Gendarmerie Law), available at: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.2803.pdf.

The Law on the Duties and Powers of Police, dated 1934 and numbered 2559 (Police Law), available at: https://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf.

The Law on the Ombudsman Institution, numbered No.6328 and dated 2012, available at: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6328.pdf.

The Law on the Right to Information, dated 2003 and numbered 4982, available at: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4982.pdf.

The Law on the State Intelligence Services and the National Intelligence Organisation, numbered 2937 and dated 1983 (MIT Law), available at: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2937&MevzuatTur=1&MevzuatTertip=5.

The Presidential Decree on Devlet Denetleme Kurulu, available at: https://www.mevzuat.gov.tr/MevzuatMetin/19.5.5.pdf.

The Regulation on Procedures and Principles Relating to Authorization to Access Providers and Hosting Providers, available at: https://www.mevzuat.gov.tr/anasayfa/MevzuatFihristDetayIframe?MevzuatTur=7&MevzuatNo=11679&MevzuatTertip=5.

Turkish Personal Data Protection Law, numbered 6698 and dated 2016, available at: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf,

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Other sources

Akman, N. G. (2021), *Protection of Personal Data by Administrative Law* (Master Thesis), available at: https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=v7BkNnnepTnbhn8rNR77LcR_II-f_TK_3XoNmW2wSHu86pEYn4zgNqFITXoQxtnR.

Alyanak, S., *The New Institution on Protection of Fundamental Rights: Turkish Ombudsman Institution*, available at: https://dspace.ankara.edu.tr/xmlui/handle/20.500.12575/42699.

Atli, T. (2019), 'KİŞİSEL VERİLERİN ÖNLEYİCİ, KORUYUCU VE İSTİHBARİ FAALİYETLER AMACIYLA İŞLENMESİ', *2 Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, available at: https://dergipark.org.tr/tr/download/article-file/747023.

[redacted]

Council of Europe, *European Court of Human Rights, Annual Report 2022*, available at: https://www.echr.coe.int/Documents/Annual_report_2022_ENG.pdf.

Council of Europe, *Interim Resolution on Execution of the judgment of the European Court of Human Rights Kavala against Turkey*, available at: https://rm.coe.int/0900001680a4b3d4.

Council of Europe, *Violations by Article and by State*, available at: https://www.echr.coe.int/Documents/Stats_violation_1959_2022_ENG.pdf.

Council of Europe Committee on Counter-Terrorism (CDCT), *Profiles on Counter-Terrorism Capacity: Türkiye*, available at: https://rm.coe.int/profile-november-2022-Türkiye/1680a94979.

Erhan, Z. (2019), *Core International Crimes In Turkish Criminal Law And The Rome Statute*, 22 Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, p. 111.

European Commission, Türkiye 2022 Report, available at https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrkiye%20Report%202022.pdf.

European Commission for Democracy Through Law (Venice Commission), *Draft Opinion on the Provisions of the Emergency Decree Law N° 674 of 1 September 2016 which Concern the Exercise of Local Democracy in Türkiye*, available at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2017)021-e.

Human Rights Action Plan (2021-2023), Circular 2021/9, available at: https://insanhaklarieylemplani.adalet.gov.tr/resimler/%C4%B0nsan_Haklar%C4%B1_Eylem_Plan%C4%B1_ve_Uygulama_Takvimi.pdf.

Human Rights Watch, *Council of Europe Sanctions Turkey*, available at: https://www.hrw.org/news/2021/12/03/council-europe-sanctions-Türkiye.

Human Rights Watch, *Türkiye Spy Agency Law Opens Door to Abuse*, available at: https://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse#:~:text=(Istanbul)%20%E2%80%93%20A%20new%20law,and%20the%20right%20to%20privacy.

Human Rights Watch, *Turkey: YouTube Precedent Threatens Free Expression*, available at: https://www.hrw.org/news/2020/12/19/turkey-youtube-precedent-threatens-free-expression.

Kaya, M. B., Tastan, F., *Kişisel Veri Koruma Hukuku: Mevzuat & İçtihat & Bibliyografya*, online, version 2.5, pp. 1774-1776, available at: https://mbkaya.com/kisisel-veri-koruma-hukuku-mevzuat-ictihat/.

Medyascope, *BTK-gate: Internet activity, identity, and personal data of all users in Turkey has been collected by BTK for the past year and a half*, available at: https://medyascope.tv/2022/07/21/btk-gate-internet-activity-identity-and-personal-data-of-all-users-in-Türkiye -has-been-collected-by-btk-for-the-past-year-and-a-half/.

OECD, *Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access*, available at: https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm#.

Olgunsoy, F. (2019), *The Impact of Intelligence Activities in Fight Against Terror on Liberties: Turkey, United Kingdom, United States of America* (PhD Thesis), available at: http://nek.istanbul.edu.tr:4444/ekos/TEZ/60634.pdf.

Personal Data Protection Supervisory Authority of Türkiye, *Bağlayıcı Şirket Kuralları Hakkında Kamuoyu Duyurusu*, 10 April 2020, available at: https://www.kvkk.gov.tr/Icerik/6728/YURT-

DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU.

Personal Data Protection Supervisory Authority of Türkiye, *International Data Transfer*, available at: https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim, https://www.kvkk.gov.tr/Icerik/4106/Kisisel-Verilerin-Yurtdisina-Aktarilmasi.

Personal Data Protection Supervisory Authority of Türkiye, *Yurtdısına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhutnamede Yer Alacak Asgari Unsurlar*, 2018, available at: https://kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-VeriSorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-AsgariUnsurlar.

Personal Data Protection Supervisory Authority of Türkiye, *5. yılında Kişisel Verileri Koruma Kurumu*, 23 November 2022, available at: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/b5731c6c-540b-45eb-a2d8-d7cef57cf197.pdf.

Ünver, H. A., Kim, G., 'Data Privacy and Surveillance in Türkiye', *EDAM Cyber Policy Paper Series 2*, 13 February 2017.

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

ANNEX 3 – ACRONYMS AND ABBREVIATIONS

General

Acronyms and Abbreviations	Meaning
CJEU	Court of Justice of the European Union
CoE	Council of Europe
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Convention 108+	Convention 108+ on protection of individuals with regard to the Processing of Personal Data
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EU	European Union
EU-Charter	Charter of Fundamental Rights of the European Union
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
HRC	United Nations Human Rights Council
HRW	Human Rights Watch
ICCPR	International Covenant on Civil and Political Rights
OECD	Organisation for Economic Co-operation and Development
SA(s)	Supervisory authority(-ies)
UDHR	Universal Declaration of Human Rights
UN	United Nations

Mexico

Acronyms and Abbreviations	Meaning
Constitution	Constituición Política de los Estados Unidos Mexicanos
ARCO	Right to access, correction, cancelation and opposition (*derechos de accesso, rectificación, cancelación u oposición*)
CNPP	Criminal Procedure Code (*Código Nacional de Procedimientos Penales, de 5 de marzo de 2014*)
INAI	National Insititute for Transparency, Access to Information and Data Protection
LFPDSSPP	Data Protection Law for Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares)*
LGPDSSO	Data Protection Law for Public Parties (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados)*
LFTAIP	Federal Law of Transparency and Access to Public Information (*Ley Federal de Transparencia y Accesso a la Información Pública*)
LGTAIP	General Law of Transparency and Access to Public Information (*Ley General de Transparencia y Acceso a la Información Pública*)
NSL	National Security Law (*Ley de Seguridad Nacional, de 31 de enero de 2005*)

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)

Türkiye

Acronyms and Abbreviations	Meaning
Constitution	The Constitution of the Republic of Türkiye
EU	European Union
CoE	Council of Europe
ECHR	European Convention of Human Rights
GNAT	Grand National Assembly of Türkiye
GDPR	General Data Protection Regulation
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
OECD	Organisation for Economic Co-operation and Development
ECtHR	European Court of Human Rights
HRW	Human Rights Watch
BTK (ICTA)	Bilgi Teknolojileri ve İletişim Kurumu (Information and Communication Technologies Authority)
TCL	Turkish Criminal Law
TPDPL	Turkish Personal Data Protection Law
SA	Personal Data Protection Supervisory Authority of Türkiye
the Board	Personal Data Protection Board
SCCs	Standard Contractual Clauses
BCR	Binding Corporate Rules
MIT	Milli İstihbarat Teşkilatı(National Intelligence Organization)
MIT Law	Law numbered 2937 on the State Intelligence Services and the National Intelligence Organization
DDK	Devlet Denetleme Kurulu(the State Supervisory Council)
TCPL	Turkish Criminal Procedure Law
AYM	Türkiye Cumhuriyeti Anayasa Mahkemesi(The Constitutional Court of Türkiye)
HTS	Historical Traffic Search

The information and views in this study are those of the author(s) and do not reflect the official opinion of the EDPB (see p. 2 for more information)