Opinion 07/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the European Patent Organisation

Adopted on 5 May 2025

Executive summary

On 4 March 2025, the European Commission started the process towards the adoption of its draft implementing decision (Draft Decision) on the adequate protection of personal data by the European Patent Organisation (EPO or Organisation)[1].

On 5 March 2025, the European Commission asked for the opinion of the European Data Protection Board (EDPB). The EDPB's assessment of the adequacy of the level of protection afforded by the EPO has been made on the basis of the examination of the Draft Decision itself as well as on the basis of an analysis of the documentation made available by the European Commission.

The EDPB focused on the assessment of the legal framework and data protection rules applicable to the EPO and legal remedies available to individuals in the European Economic Area (EEA), including the access by public authorities to personal data transferred from the EEA to the EPO.

The EDPB also assessed whether the safeguards provided under the EPO legal framework are in place and effective, and focused its assessment particularly on the oversight and enforcement, taking into account the specificities of international organisations.

The EDPB has used as main reference for this work the Adequacy Referential adopted by the Article 29 Working Party[2].

The EDPB positively notes that the EPO data protection framework presents numerous similarities to the European Union data protection framework, including on data protection rights and principles.

It has also concluded that certain aspects should be further clarified, and closely monitored by the European Commission.

In particular, the EDPB invites the Commission to clarify that, in the context of the data protection governance structure implemented by the EPO, the controller (i.e. European Patent Office) remains the entity ultimately responsible for infringements of the data protection rules.

With regard to onward transfers, the EDPB observes that the requirement to not undermine the level of protection is not expressly mentioned in connection with the so-called "transmissions" of personal data to public authorities in EPO contracting states. The EDPB asks the Commission to clarify this point and to clarify what safeguards apply when personal data are transmitted in the specific context of the patent granting procedure.

Given the close connection between the Data Protection Officer (DPO) and the Data Protection Board (DPB), as well as the importance of investigative, auditing and corrective powers, the EDPB recommends the Commission to further clarify the interplay between them, notably with regard to the exercise of investigative, auditing, and corrective powers, as well as to clarify the role of the DPO in handling data subjects' request, and its role, if any, in the complaints procedure before the DPB. Furthermore, the EDPB notes that the DPB's (reasoned) opinions issued in the context of the complaints procedure remain non-binding and invites the Commission to verify and ensure that the DPB's powers are binding in this context, and to assess whether additional safeguards could be provided for to this end.

[1] Press release https://ec.europa.eu/commission/presscorner/detail/sv/ip_25_613 .
[2] Article 29 Working Party, WP 254 rev.01, adopted on 28 November 2017 and as last revised and adopted on 6 February 2018, endorsed by the EDPB.

The EDPB has also analysed the EPO's legal framework with respect to public authorities' access and use of personal data transferred from the Union to the Organisation. In this regard, the EDPB highlights that the assessment of government access in the present case is distinct from the corresponding assessment of the level of protection afforded by a third country. The specific scenario of a decision on the adequate protection of personal data by an international organisation requires reviewing the rules that determine how that organisation processes governmental access requests.

Regarding contracting states, the EPO's immunities are complemented by a duty of cooperation. To this end, the EPO may waive its immunity from jurisdiction and execution to respond to governmental access requests. The EDPB calls on the Commission to further clarify, particularly with a view to access requests for law enforcement and national security purposes, how the obligation to cooperate relates to the concept of immunity. In this context, the EDPB invites the Commission to also clarify the President's authority and scope of discretion when deciding on a request for cooperation.

If the EPO chooses to comply with a request for access from a contracting state, the requirements for transmissions apply. These rules are applicable to all contracting states, regardless of whether the contracting state is an EEA member state or qualifies as a third country from an EU data protection law perspective. The EDPB underlines that the requirements of Chapter V GDPR, to the extent required to establish essential equivalence, need to be sufficiently addressed and invites the Commission to clarify what safeguards apply in such cases.

Table of contents

The European Data Protection Board

Having regard to Article 70(1)(s) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter GDPR),

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

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

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

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

2. The EDPB recalls that adequacy decisions ensure the continuous protection of personal data transferred from the EEA to third countries and are a robust transfer tool to ensure the data subject's rights are safeguarded when data are transferred outside the EEA.

3. In particular, the EDPB welcomes the Commission's initiative to work on the first adequacy decision for an international organisation, and underlines the importance of this decision to demonstrate that the legal framework of international organisations can be recognised as ensuring an adequate level of protection within the meaning of Article 45 GDPR.

4. The EDPB takes this opportunity to encourage the Commission to continue dialogues with international organisations in order to develop, expand and multiply this kind of adequacy decisions along with the ones relating to third countries.

1.1 Structure and data protection framework of EPO

5. The European Patent Organisation, headquartered in Munich, is an intergovernmental organisation established by the European Patent Convention (EPC)[4]. It has 39 contracting states and possesses legal personality. It comprises two main organs: the European Patent Office (Office), which functions as its executive arm, and the Administrative Council, which exercises legislative powers on behalf of the EPO and is responsible for policy issues (Article 33 EPC).

[3] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".
[4] Recital (7) of the Draft Decision.

6. The EPO's main competence is to grant European patents, a task carried out by the Office under the supervision of the Administrative Council.

7. The President represents the EPO and is the head of the Office which includes various departments. The President is responsible for managing the Office's operations and for disciplinary matters, and is accountable to the Administrative Council. The Administrative Council is composed of representatives from the contracting states, oversees policy matters and the Office's activities.

8. On 30 June 2021, the EPO adopted the Data Protection Rules (DPR) which implement Articles 1B and 32A of the Service Regulations[5], and are applicable to the processing of personal data by the Office[6].

9. The DPR are supplemented by instruments issued by the President, in particular circulars, internal administrative instructions, and decisions (such as the decision on countries and entities ensuring adequate data protection (17 November 2022), and the "*Circular No. 420 Implementing Article 25 of the Data Protection Rules (DPR) on restriction of data subjects' rights*"). All these instruments are legally binding[7].

10. The DPR are further supplemented by operational documents issued by the Data Protection Officer, which specify more detailed requirements and procedures for processing of personal data (Article 1(2)(c) DPR). Such operational documents are part of the EPO data protection framework and as such legally binding, and are available to data subjects on the EPO's website.

1.2 Specificities of International Organisations

11. Pursuant to Article 4(26) of the GDPR an international organisation (IO) is "*an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries"*. Under international law, the status of international organisations is similar to that of sovereign states; however, according to the principle of functional immunity, international organisations enjoy privileges and immunities only to the extent necessary for the exercise of the functions they have been created to carry out[8]. "Privileges" generally include exemptions from the substantive law of a state (e.g. tax and customs exemptions) whereas "immunities" are exemptions from legal process, execution and enforcement measures.

12. The source of privileges and immunities of IOs can be: multilateral treaties, international agreements creating the IO, headquarter agreements with the hosting state, and domestic law and legislation. Privileges and immunities are usually recognised by the states which are members of the organisations, unless third countries have explicitly or implicitly recognised the international organisation in domestic

[5] The Service Regulations regulate aspects relating to the EPO's staff, including staff rights and obligations. See in this regards Article 33 EPC. The EPC is available at the following link https://link.epo.org/web/EPC_17th_edition_2020_en.pdf.

[6] Processing of personal data carried out by the Administrative Council of the EPO are governed by the Administrative Council Data Protection Rules (AC DPR) whereas processing of personal data carried out by the Select Committee are governed by the Select Committee Data Protection Rules (SC DPR). The AC DPR and the SC DPR respectively establish the application of the DPR to processing of personal data carried out by the Administrative Council and by the Select Committee, with the necessary modifications. Article 145 EPC clarifies the role of the Select Committee.

[7] Article 10 EPC, Article 1(2)(a) DPR, and Article 3(y) DPR.

[8] Christopher Kuner: International Organizations and the EU General Data Protection Regulation, University of Cambridge Faculty of Law Legal Studies Research Paper Series, Paper 20/2018.

law. However, immunity from national jurisdiction is not absolute and requires that individuals have reasonable alternative means to effectively protect their rights[9].

1.3 EPO's Privileges and Immunities

13. The Privileges and Immunities enjoyed by the EPO are regulated by the "*Protocol on Privileges and Immunities of the European Patent Organisation*" (PPI) and covers, among others, premises of the EPO (Article 1); inviolability of archives (Article 2 PPI); jurisdiction and execution (Article 3 (1)(a) PPI), property and assets of the EPO: except in so far as may be temporarily necessary in connection with the prevention of, and investigation into, accidents involving motor vehicles belonging to or operated on behalf of the Organisation. (Article 3(3) PPI); tax exemption (Article 4 PPI).

14. EPO's immunities are complemented by a duty of cooperation between the EPO and public authorities of the contracting states as set out in Article 20 PPI. In addition, according to Article 19 (2), the President of the European Patent Office has the duty to waive immunity where he considers that such immunity prevents the normal course of justice and that it is possible to dispense with such immunity without prejudicing the interests of the Organisation.

1.4 Data protection governance of EPO

15. According to Article 3(g) DPR, the European Patent Office acts as controller[10]. The EPO data protection framework foresees the possibility for the controller to identify operational units as "delegated controllers" (Article 28(3) DPR). According to Article 3(h) DPR "*delegated controller means the operational unit, represented by its head, ensuring that all processing operations involving personal data that are performed within the operational unit comply with these Rules. The person representing the unit shall be a manager at senior level, normally at least a principal director*".

16. The EDPB observes that this internal governance structure is common in the context of international organisations[11] given the size and nature of IOs' work. Similarly, companies benefit from having an internal structure to support compliance with data protection rules[12].

17. However, the EDPB notes that the ultimate responsibility in case of infringement of the data protection rules should remain with the controller (i.e. the European Patent Office)[13]. In light of the above, the EDPB invites the Commission to further clarify this point.

2. GENERAL DATA PROTECTION ASPECTS

2.1 Content principles

[9]Waite and Kennedy ECtHR v. Germany, Appl. No. 26083/94, Judgment of February 18, 1999, paras from 67 to 73.

[10] Article 28 DPR further details the controllership within the EPO.

[11] For instance, Eurocontrol's DP regulation refers to 'internal controllers' https://www.eurocontrol.int/sites/default/files/2024-05/eurocontrol-regulation-personal-data-protection-2024.pdf; the EIB uses the term controller both for the delegated controllers and the EIB, but the text often refers to 'relevant controllers' making clear that they concern a specific entity within the EIB available at https://www.eib.org/attachments/lucalli/20220237_data_protection_rules_implementing_eu_regulation_en.pdf

[12] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.1, adopted on 07 July 2021.

[13] Ibid., paras 17 and 18.

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

19. The EDPB welcomes the recognition of the rights to privacy and to data protection as fundamental rights according to the DPR.

2.1.1 Concepts

20. The EDPB acknowledges that the terminology used in the EPO data protection framework is consistent with that of the EU data protection framework. This alignment is a positive factor that, while not a prerequisite for equivalence, merits recognition.

21. As regards to the concepts of "delegated controller" and of "operational unit", and their practical consequences, the EDPB refers to section 1.4, above.

2.1.2 Data protection principles

22. The data protection principles laid down in Articles 4(2) and 6 DPR are very similar to those set out in Articles 5 and 6(4) GDPR, respectively. Similarly, the legal bases for processing that are set out in Articles 5, 7, 11 and 12 DPR mirror the legal bases set out in Article 6 GDPR and the conditions in Articles 9 and 10 GDPR[14].

23. Pursuant to Article 11(2) DPR, special categories of personal data can be processed under very similar conditions as those set out under article 9 GDPR, except for certain cases stemming from the nature of the EPO. Under Article 11(2)(f) DPR, for instance, such data can be processed when it is necessary for a specific purpose relating to the performance of a task carried out in the exercise of the official activities of the Organisation or in the legitimate exercise of the official authority vested in the controller.

24. In such cases, however, Article 11(2)(f) DPR provides specific measures to ensure that the level of protection of the special categories of personal data is not undermined.

25. The EDPB welcomes that, in relation to the purpose limitation principle, the compatibility of further purposes is understood similarly in both Articles 4(2)(b) and 6 DPR as in Articles 5(1)(b) and 6(4) GDPR.

26. Furthermore, the EDPB welcomes the inclusion of the accountability principle in Article 4(1) DPR, and of measures necessary to demonstrate compliance, such as the keeping of records (Article 32), data breach notification obligations (Article 34), data protection impacts assessment (Article 38 DPR) as well as the inclusion of privacy by design and by default (Article 27(1) and (2) DPR), which also ensure compliance with the data minimisation and necessity principles. The EDPB positively notes that such principles and obligations are very similar to those laid down under the GDPR.

27. Additionally, the EDPB welcomes that Article 4(1) DPR states that the controller shall actively and continuously implement measures to ensure the protection of personal data in their processing

[14] See recitals from 26 to 29 of the Draft Decision.

activities, thereby making them responsible for compliance with data protection laws and requiring them to demonstrate this compliance to data subjects at all times.

2.2 Individual rights

28. The EDPB welcomes that the DPR provide individuals with the same rights as those laid down in the GDPR (Articles 12 to 22), namely the right of access (Article 18 DPR), the right to rectification (Article 19 DPR), the right to erasure (Article 20 DPR), the right to restriction of processing (Article 21 DPR), the right to data portability (Article 22 DPR), the right to object (Article 23 DPR) and the right not to be subject to automated decision-making (Article 24 DPR). In the same way, the right to be informed about the restriction of data subject rights (Article 23 (2)(h) GDPR) is recognised by Article 7 of Circular No. 420 issued by the President of the EPO.

29. Similarly to Article 23 GDPR, Article 25 DPR states that certain legal provisions within EPO's legal framework may restrict the application of the rights outlined in Article 18 to 25 DPR and provides for the minimum content that the measures providing for the restrictions should include. Such minimum content mirrors the one required by the GDPR. In addition, any assessment of the need for restriction shall be duly documented.

30. So far, the EPO has implemented this provision by means of Circular No. 420, which clarifies what rights can be restricted and for which objectives. It also clarifies that the restriction shall be temporary and that it is for the controller to determine whether, depending on the relevant circumstances, the restriction applies. In doing so, the controller shall carry out a case-by-case necessity and proportionality test, which has to be documented and communicated to the EPO DPO. The DPO has the power to request the review of a restriction and the data controller has to inform in writing of the outcome of the review.

31. The EDPB positively notes that according to Article 25(2) and (4) DPR, and Article 7 Circular No. 420, data subjects have to be informed about the restrictions, unless this would cancel the effect of the restriction (in line with Article 23 GDPR and Article 25 EUDPR), and about their right to consult the DPO with a view to challenging the restrictions and their rights under Article 49 and 50 DPR (Article 25(3)(b) DPR). In this context, the EDPB welcomes that the information on restrictions of data subjects' rights is available on the EPO website in compliance with Article 7 Circular No. 420.

32. In addition, the EDPB observes that a number of limitations of data subjects' rights are in place due to the EPO's tasks. The EPO, for instance, has a duty to maintain the European Patent Register where certain legally defined personal data are published. Likewise, the right to rectification and deletion are limited: the EPO cannot provide for the rectification of information - including personal data - contained in documents used in the patent granting procedure (as it is the case for documents belonging to official and legal proceedings, such as a statement of claim or a responding statement) and the EPO has to follow specific retention periods and publication requirements for certain documents used in the patent granting procedure (Article 129(a) EPC).

33. The EDPB notes that restrictions of data subjects' rights provided by the EPO are limited to what is strictly necessary and proportionate to ensuring the correct functioning of the patent granting procedure, thereby respecting the essence of the fundamental rights and freedom of data subjects, and the necessity and proportionality requirements as set out in the Charter of Fundamental Rights of the European Union (Charter) and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

2.3 Restrictions on onward transfers

34. The GDPR Adequacy Referential clarifies that the level of protection of natural persons whose personal data is transferred under an adequacy decision must not be undermined by the onward transfer and therefore any onward transfer "should be permitted only where the further recipient (i.e., the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller"[15]. While the DPR distinguishes between so-called "transmissions of personal data" and "transfers of personal data" and provides for different rules for these two categories of transfers[16], the EDPB underlines that the requirement to not undermine the level of protection applies to all onward transfers of personal data transferred from the EU, irrespective of the terminology used.

35. The EDPB observes that rules very similar to those of Chapter V GDPR apply to the "transfers of personal data" (as defined under Article 3(t) DPR) in order to ensure that the level of protection guaranteed by the DPR is not undermined (Articles 9 and 10 DPR).

36. The EDPB welcomes this close alignment with Chapter V GDPR and positively notes the reference in the DPO transfer guidance to EDPB Guidelines and developments within the Union framework[17] .

37. In light of the above, the EDPB has focused its assessment on the rules applicable to the other category of transfers under the DPR, the "transmissions of personal data".

2.3.1 Transmissions of personal data

38. According to Article 3(s) DPR "transmissions of personal data" refer to the "disclosure, dissemination of or otherwise making available, including by granting access, of personal data to a party within the European Patent Organisation or to a national industrial property office or other public authority of a contracting state to the European Patent Convention under the conditions laid down in Article 8".

39. Article 8(1) DPR stipulates that transmissions of personal data to a public authority of an EPO contracting State may occur if the data are necessary for the performance of that public authority's tasks and if the transmission is compatible with the tasks and functioning of the EPO[18]. Article 8(2) DPR allows for transmission of personal data to a national industrial property office of an EPO contracting state if the data are necessary for the performance of tasks within the recipient's competence and if the exercise of its official authority and processing is necessary to carry out tasks in the exercise of the official activities of the EPO or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the EPO's management and functioning. Such transmissions take place in the context of the patent granting procedure provided for under the EPC and the PCT[19].

---

[15] Article 29 Working Party, WP 254 rev.01, adopted on 28 November 2017 and as last revised and adopted on 6 February 2018, endorsed by the EDPB, Chapter 3, A.9.
[16] See recitals 62-72 of the Draft Decision.
[17] EPO transmission and transfer of personal data, Explanatory Note, Version of January 2024, part 3.2 (p. 9).
[18] See recital 63 of the Draft Decision; this could be for the purpose of cooperation through consultation processes; secondment and deployment of experts; providing information on EPO staff for the purpose of determining social benefits, tax requirements, etc.
[19] See recital 62, footnote 165, of the Draft Decision and OJ EPO 2021, A98 – Decision of the President of the European Patent Office dated 13 December 2021 concerning the processing of personal data in patent-grant and related proceedings.

40. Recipients shall provide evidence that it is necessary to have the data transmitted for a specific purpose deriving from the EPO's obligations of co-operation with the contracting state, and the controller - where the legitimate interests of the data subject might be affected - shall establish that it is proportionate to transmit the data for that specific purpose, after having demonstrably weighed up the competing interests (Article 8(3) and 8(4) DPR).

41. To provide appropriate guarantees as tools for transmissions, specific data protection provisions should be inserted into enforceable instruments, such as memoranda of understanding (MoU) or administrative arrangements[20]. The EPO DPO has prepared model data protection clauses for MoUs providing *inter alia* for data protection principles, including for example purpose limitation, data subject rights as well as independent oversight and appropriate enforcement mechanisms.[21] The EDPB acknowledges the provision of such safeguards but notes, however, that the requirement to not undermine the level of protection is not specifically mentioned in relation to transmissions, neither in Article 8 DPR nor in the EPO Explanatory Note on transmission and transfer of personal data or in the draft adequacy decision. The EDPB observes that, in contrast, this requirement is expressly mentioned in the context of transfers[22], and asks the Commission to clarify this point.

42. Moreover, the EDPB has understood from additional explanations given by the Commission that the requirement for appropriate guarantees as tools for transmissions does not apply where the recipient is a national industrial property office. Consequently, it is not fully clear to the EDPB what data protection safeguards apply when personal data are transmitted in the context of the patent granting procedure. The EDPB, therefore, invites the Commission to also clarify this point.

2.4 Procedural and enforcement mechanisms

43. According to the Adequacy Referential[23], and to the relevant case-law of the CJEU[24], a data protection system essentially equivalent with the European Union model must provide for: (i) an independent authority, which should oversee and enforce data protection laws, with the power to investigate and take action without external influence. The data protection systems must ensure (ii) that data controllers and processors are accountable and aware of their responsibilities, while data subjects are informed of their rights. Effective sanctions and verification processes should be in place to ensure adherence to rules; (iii) that data controllers and processors demonstrate compliance, through measures like data protection impact assessments, records of processing activities, and the appointment of data protection officers. In addition, (iv) the data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms.

44. As regards the accountability principle covering point (ii), and (iii) of the previous paragraph, the EDPB refers to Section 2.1.2 above.

45. In the next sections, the EDPB has focused its assessment on the existence of an independent authority and of an appropriate redress mechanisms.

[20] EPO transmission and transfer of personal data, Explanatory Note, Version of January 2024, p. 6.
[21] Overview of the requirements of the EPO's model data protection clause for Memoranda of Understanding, Version of June 2024.
[22] See recital 67 of the Draft Decision.
[23] Article 29 Working Party, WP 254 rev.01, adopted on 28 November 2017 and as last revised and adopted on 6 February 2018, endorsed by the EDPB, Chapter 3, C.
[24] CJEU, October 6, 2015, Judgment in case C-362/14, Maximillian Schrems v Data Protection Commissioner ("Schrems").

2.4.1 Data Protection Officer and Data Protection Board

46. The system presented by the EPO establishes two distinct bodies responsible for the oversight of compliance with the data protection rules: the Data Protection Officer and the Data Protection Board (Article 32A of the Service Regulations).

47. The EPO Data Protection Officer, in addition to fulfilling the traditional role of the DPO under the GDPR, also holds investigative powers according to Article 43 DPR.

48. The DPB's role is to ensure independent, effective and impartial oversight of the data protection rules. Data subjects have the right to file a complaint before the DPB in case of disagreement with a decision or an implicit rejection of a request for review by a delegated controller of a request for review by a delegated controller (Article 50 DPR).

49. While this dual structure, justifiable by the EPO's nature, is not inherently concerning or problematic, it is essential that both bodies operate with full independence to ensure effective oversight and enforcement, and that they have all necessary powers to carry out their tasks.

50. In this regard, the EDPB has focused its assessment on the actual independence of these oversight bodies, and on their powers. As regards independence, the EDPB welcomes not only the language supporting this principle in the relevant Articles, but also the additional safeguards in place.

51. Within this framework, the EDPB has examined the rules governing the appointment, removal, and dismissal of the DPO and of the DPB, particularly the requirement for the President to consult the DPB prior to any proposed removal or dismissal of the DPO.

52. The EDPB considers this prior consultation a potential safeguard for the DPO's independence, however the nature and implications of such consultation remain unclear. Therefore, the EDPB invites the Commission to further clarify this point and to consider monitoring, during future reviews, that in practice the DPO is not dismissed or penalised by the controller for the performance of its duties.

53. The EDPB observes that pursuant to Article 47 DPR, the DPB has an oversight and advisory function as the DPB advises the controller and the delegated controllers in relation to the application of Articles 38 and 39 DPR, advises on the dismissal of the Data Protection Officer under Article 48(2) DPR, and provides an opinion on the use of the mechanism for legal redress under Article 50.

54. Concerning the appointment of the members of the DPB, the EDPB notes that pursuant to Article 48(1) DPR, the Data Protection Board is composed of three external experts in the field of data protection appointed by the President of the Office, namely a chair and two other members, one of whom acts as deputy chair. According to Article 48(2) DPR, the chair, the two other members and the alternate members of the DPB shall have the qualifications required for appointment to judicial office or be data protection professionals with proven expertise and experience in the area.

55. The EDPB welcomes that rules for the selection of the members of the oversight body require data protection expertise, and encourages the Commission to monitor that members of the DPB selected for their qualifications have the necessary level of data protection expertise given its importance for the oversight function.

2.4.2 Investigative and corrective powers

56. In this context the CJEU clarified that powers of supervisory authorities constitute necessary means to perform their duties, and they should possess in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers

of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings[25].

57. According to Article 43(1)(d), the DPO can carry out data protection audits (DP Audits) and investigations (conducted in the form of DP Inspections or Ad hoc Queries)[26]. According to the "Data Protection Oversight" note[27], which further details Article 43 DPR, the DPO, in consultation with the DPB, prepares an annual data protection audit plan (Plan) and submits the same to the President of the EPO for approval. The approved Plan is submitted to the DPB for information. The DPB can, at any time, formulate suggestions on areas on which the Office should perform a DP Audit.

58. Pursuant to Article 43(1)(i) DPR, the DPO has to respond to request from the Data Protection Board, and to cooperate and consult with the DPB at its request or on his or her own initiative. According to Article 43(1)(j) DPR, the DPO has to facilitate the cooperation between the Data Protection Board and the Office concerning - among others - data protection investigations, complaint handling, data protection impact assessments and prior consultations. The DPO also has to forward to the DPB information on new administrative measures and internal rules relating to the processing of personal data.

59. The DPO fills in a report of the investigations and audits carried out, and in case it identifies non-compliance with the data protection rules, the report shall include its findings, conclusions and recommendations (including remedial measures).

60. In particular, according to the "Data Protection Oversight" note the recommendations can include "preventive, mitigating or corrective measures" for the controller in case of irregularity or incompliance. The DPO may recommend to bring processing operations in compliance with the DPR; to comply with data subjects' requests to exercise their rights under the DPR; to communicate a personal data breach to the data subject(s); to suspend a particular data processing operation; or that the data flow to specific recipients is suspended[28].

61. In line with the "Data Protection Oversight" note and with the Decision of the President of the Office dated 12.07.202429, the conclusions and recommendations may become binding (subject to the Board's validation) and must be implemented by the controller. According to Data Protection Oversight note, which further details rules contained in Article 43(1)(i) and (j) DPR, the DPB has the power to comment on conclusions and recommendations and also to ask for changes, which the DPO shall implement. Furthermore, the DPO has the authority to initiate follow-up inspections or extend the scope of the data protection inspections, and to recommend to launch administrative investigation to determine whether disciplinary or other measures action is needed.

---

[25] CJEU, October 6, 2015, Judgment in case C-362/14, Maximillian Schrems v Data Protection Commissioner ("Schrems"), para 43.

[26] The investigative powers of the DPO are further detailed in the "Data Protection Oversight - How the Data Protection Office conducts DP Audits and DP Inspections", available on the EPO website at the following link https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

[27] "Data Protection Oversight - How the Data Protection Office conducts DP Audits and DP Inspections", available on the EPO website at the following link https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

[28] Ibid.

[29] Decision of the President of the Office on the Enforceability of DPO Recommendations endorsed by the Data Protection Board in the framework of Data Protection Audits and Inspections Conclusions available at the following link https://link.epo.org/web/office/data-protection-and-privacy/en-decision-of-the-president-on-enforceability-of-dpo-conclusions-and-recommendations.pdf.

62. Given the close connection between the DPO and the DPB, as well as the importance of investigative, auditing and corrective powers, the EDPB recommends the Commission to further clarify the interplay between them, notably with regard to the exercise of investigative, auditing, and corrective powers, as well as to clarify the role of the DPO in handling data subjects' request (Article 43(1)(k) DPR), and its role, if any, in the complaints procedure in front of the DPB according to Article 50 DPR. In particular, the EDPB invites the Commission to monitor that it is clearly distinguished in practice when the DPO acts on its own behalf (performing its role and function as DPO) and when it is acting on behalf of the DPB to support the latter in the performing of its oversight functions. This would provide additional clarity on the oversight structure and on the roles of the DPO and the DPB.

2.4.3 Complaints procedure before the Data Protection Board

63. The EDPB observes that data subjects have the right to lodge a complaint before the Data Protection Board which handles it in line with the procedure set out in Article 50 DPR, and the Rules of Procedure set out in Annex 1 of the DPR.

64. In particular, after examining the complaint, the DPB issues a reasoned opinion to the controller, where it may recommend that compensation for material or non-material damage is awarded.

65. According to Article 50(4) DPR, the DPB's reasoned opinions (hereinafter also opinion) are not binding on the controller which may choose not to comply with them. In such a case, the controller must provide a written explanation, and it is also asked to notify the data subject, the delegated controller and, where applicable the processor, the DPO, and the DPB, of its final decision and the conclusions of the DPB. The decision (constituted by the DPB's reasoned opinion and the final decision of the controller) can be challenged by the data subject by requesting the President of the Office to initiate the arbitration procedure set forth by Article 52 DPR or via the Administrative Tribunal of the International Labour Organisation.

66. According to the EDPB Guidelines, the Adequacy Referential and the case-law of the CJEU, the oversight body shall have binding powers as this is a key factor in ensuring the effectiveness of the supervision mechanism.

67. The EDPB notes that the DPB's opinions issued in the context of complaints handling remain non-binding. While the conclusions and recommendations of the DPO — following investigations and audits, which may have been initiated at the DPB's request — can become binding upon the DPB approval, they do not appear to apply to cases initiated under Article 50 GDPR, i.e. data subjects' complaints.

68. In light of the above, the EDPB invites the Commission to verify and ensure that the DPB's powers are binding in the context of complaints handling pursuant to Article 50 DPR, and to assess whether additional safeguards could be provided for to this end.

69. However, the EDPB welcomes that the decisions of the controller pursuant to Article 50(6) DPR can be appealed, as this provides data subjects with a necessary redress mechanisms and enables the enforcement of the oversight body's decision.

70. Additionally, the EDPB welcomes that also the DPB may recommend that compensation for material or non-material damage be awarded (Article 50(3) DPR).

2.4.4 Redress mechanisms and arbitration

71. According to the Adequacy Referential, data subjects should be provided with effective redress, including compensation for damages as a result of the unlawful processing of their personal data. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

72. The EDPB notes that, according to the EPO's data protection framework, data subjects have the right to request a review of the processing of their personal data before the delegated controllers when they believe a violation of data protection rules has occurred. This serves as a prerequisite for filing a complaint with the DPB as independent oversight body pursuant to Article 50 DPR. This requirement represents a novel feature compared to the EU data protection system, which however does not undermine the level of protection afforded by the EPO system as it affects neither the enforceability of data subjects' rights nor their right to compensation.

73. According to Article 50 and 52(1) DPR, when data subjects are not satisfied with the final decision following the procedure under Article 50 DPR, they can appeal it. Employees of the EPO can challenge the decision via the Administrative Tribunal of the International Labour Organisation. Any other data subject has three months to submit a request to the President for arbitration.

74. The EDPB welcomes the provisions of a redress mechanism. As regards the arbitration mechanism, the EDPB notes that it is possible to provide for alternative dispute resolution mechanisms, when judicial mechanisms are not available, due, for instance, to the controller's status as international organisation. Those alternative dispute resolution mechanisms must offer the data subject guarantees essentially equivalent to those required by Article 47 of the Charter[30]. Therefore, the provision of an alternative mechanism does not per se present any inherent concerns or issues[31] provided that the arbitration (i) guarantees an independent and impartial adjudication in accordance with the principles of due process, (ii) is binding on the controller (EPO)[32], allows (iii) for compensation, and (iv) for the imposition of sanctions where appropriate.

75. Similarly, the European Court of Human Rights has ruled that effective remedies can be provided through "reasonable alternative means" such as arbitration [33] .

76. The EDPB positively notes that the EPO legal framework foresees (i) rules to ensure the independence of the arbitrator (Article 52(3) DPR), (ii) the binding nature of the arbitration mechanism (Article 52(1) DPR), as well as (iii) the right to compensation for damages suffered as a result of an infringement of the data protection rules (Article 53 DPR) and (iv) the imposition of sanctions where appropriate (Article 11 of the Arbitration Rules of the European Court of Arbitration[34]).

---

[30] CJEU July 16, 2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), paras 96 and 186 and seq.

[31] Article 29 Working Party Adequacy Referential Adopted on 28 November 2017 As last Revised and Adopted on 6 February 2018; Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies Version 2.0 Adopted on 15 December 2020, para 53, and para 75.

[32] CJEU, October 6, 2015, Judgment in case C-362/14, Maximillian Schrems v Data Protection Commissioner ("Schrems"), paras 41 and 95; CJEU July 16, 2020, Judgment in case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), paras 186,187,189, 195 and seq.

[33] ECthR, Fifth Section, Decision, Application no. 415/07. Roland KLAUSECKER vs Germany available at the following link https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-151029%22.

[34] The Arbitration Rules of the European Court of Arbitration are available at the following link https://cour-europe-arbitrage.org/arbitration-rules/

77. Furthermore, the EDPB welcomes the fact that the costs of the arbitration are borne by the EPO, thereby meeting the requirement that legal remedies to enforce data subjects' rights must not involve prohibitive costs[35].

3. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE UNION TO THE EUROPEAN PATENT ORGANISATION BY PUBLIC AUTHORITIES

78. The EDPB highlights, as a preliminary matter, that the assessment of public authorities' access and use of personal data transferred from the Union in the present case is distinct from the corresponding assessment of the level of protection afforded by a third country. Rather than evaluating the relevant third country laws and practices on government access, the specific scenario of a decision on the adequate protection of personal data by an international organisation requires reviewing the rules that determine how that organisation processes governmental requests for access to personal data including, in particular, the possibility and the rules for refusing such requests. Therefore, the standard against which essential equivalence is assessed, differs, with respect to governmental access to data, from previous adequacy decisions.

79. As a further general comment upfront, the EDPB notes that, according to additional explanations from the Commission, the EPO has not yet received any request for access to data for law enforcement or national security purposes.

80. The fact that to date no requests for law enforcement or national security purposes have been filed with the EPO implies that the rules applicable in such cases have, in this respect, not yet been put to the test in practice. Thus, the EDPB encourages the Commission to monitor whether the EPO receives any such requests in the future and how the relevant rules are implemented in the specific context. The Commission could examine, in particular, how the EPO rules and standards apply for law enforcement and intelligence agencies request, such as the requirement to provide evidence that it is necessary to transmit data for a specific purpose deriving from the EPO's obligation to cooperate (Article 8(3) DPR). Such evidence will in turn be the basis for the EPO's review of whether a transmission is necessary and proportionate (Article 8(4) DPR)[36].

3.1 Processing of governmental requests for access to personal data by EPO

81. The Draft Decision outlines that the legal framework under which the EPO assesses and responds to requests from public authorities concerning personal data follows from the PPI, the DPR requirements on transmissions and transfers of personal data, and public international law[37]. While this framework applies generally to requests both from contracting and non-contracting states, the specific provisions establish a different regime for requests issued by public authorities of contracting states, on the one hand, and of non-contracting states, on the other.

82. Regarding contracting states, the EPO's immunities that are laid down in the PPI (see paragraph 14) are complemented by a duty of cooperation. Article 20(1) PPI stipulates that the EPO "*shall co-operate at all times with the competent authorities of the Contracting States in order to facilitate the proper*

[35] Article 29 Working Party, WP 254 rev.01, adopted on 28 November 2017 and as last revised and adopted on 6 February 2018, endorsed by the EDPB, para 4.
[36] On the legal framework for transmissions see also above paragraphs 56 and 57 of this opinion.
[37] See recital 96 of the Draft Decision.

administration of justice, to ensure the observance of police regulations and regulations concerning public health, labour inspection or other similar national legislation, and to prevent any abuse of the privileges, immunities and facilities provided for in this Protocol"[38]. To this end and as provided for in Article 3(1)(a) PPI, the EPO may waive its immunity from jurisdiction and execution to respond to governmental access requests. The EDPB duly notes that it indeed appears inevitable to provide for cooperation mechanisms with public authorities from contracting states, which in certain cases may even serve the interests of the data subject, e. g., when concerning social benefits and insurance matters of the EPO staff. However, Article 20(1) PPI raises the question, particularly with a view to access requests for law enforcement and national security purposes, of how the obligation to cooperate relates to, or interacts with, the concept of immunity. The Commission has indicated that EPO's rules on cooperation shall be understood as part of the broader general principle of immunity, and therefore the EPO would be in a position to reject requests for the aforementioned purposes, irrespective of Article 20(1) PPI. The EDPB calls on the Commission to further clarify this point in the decision.

83. The decision on a request for cooperation lies with the President of the Office, who, as the Draft Decision indicates, exercises discretion in doing so[39]. While the Draft Decision refers to Article 3(1)(a) PPI as the legal basis for waiving the Organisation's immunity, it does not clearly identify a provision vesting the President with the discretion at issue and setting forth the criteria guiding the exercise of such discretion when deciding on a request for cooperation. The EDPB notes that, under Article 19(2) PPI, the President "has the duty to waive immunity where he considers that such immunity prevents the normal course of justice and that it is possible to dispense with such immunity without prejudicing the interests of the Organisation". This requirement raises additional questions about the scope of the President's discretion. Further to the previous paragraph, the EDPB thus invites the Commission to clarify these aspects in the decision.

84. If the EPO chooses to comply with a request for access from a contracting state in line with Article 20(1) PPI, the DPR requirements for transmissions apply (see paragraphs 38 et seq.)[40]. These rules are applicable to all contracting states, regardless of whether the contracting state is an EEA member state or qualifies as a third country from an EU data protection law perspective. However, the rules for transmissions, in contrast to the regime for transfers to public authorities outside of EPO's contracting states, do not explicitly require that an adequate level of protection for the data transferred be ensured in the recipient country[41]. In this regard, the EDPB wishes to recall its Guidelines on Article 48 GDPR[42], which specify that "*where data processed in the EU are transferred or disclosed in response to a request from a third country authority, such disclosure is subject to the GDPR and constitutes a transfer within the meaning of Chapter V. This means that, as for any transfer subject to the GDPR, there has to be a legal basis for the processing in Article 6 and a ground for transfer in Chapter V*".[43] In this regard, the EDPB reaffirms its request for clarification expressed in paragraph 41 above and invites the Commission to clarify what safeguards apply also with a view to transmissions based on governmental access requests, in particular requests for law enforcement and national security purposes. It should be ensured that the requirements of Chapter V GDPR, to the extent required to

[38] According to additional information provided by the Commission, the EPO so far has not applied the authority under Articles 20(2), 25 PPI to conclude complementary agreements with one or more contracting states for law enforcement or national security purposes.
[39] See recital 97 of the Draft Decision.
[40] Ibid.
[41] See recitals 63-65 of the Draft Decision and Article 8 DPR.
[42] EDPB Guidelines 02/2024 on Article 48 GDPR, adopted on 02 December 2024.
[43] Ibid, para 9.

establish essential equivalence, are sufficiently addressed, including where the concept of third countries in EU data protection law and the EPO legal framework do not fully coincide[44].

85. While the EDPB recognises that the EPO Explanatory Note on transmission and transfer of personal data states that "*to provide appropriate guarantees as tools for transmissions, specific data protection provisions should be inserted into enforceable instruments, such as, memoranda of understanding or administrative arrangements*"[45] it may not be feasible, in practice, to implement such tools vis- à-vis law enforcement authorities and national security agencies. The EDPB considers that transmissions of personal data to contracting but non-EEA member states, notably for law enforcement and national security purposes, would thus require particular attention by the Commission.

86. As there is no legal instrument that specifically regulates the processing of requests from public authorities of non-contracting states by EPO, the general rules for transfers under the DPR apply, which are very similar to those of Chapter V GDPR (see paragraphs 35 and 36).

3.2 Restriction of data subject rights

87. Article 25 DPR foresees that specific legal provisions in the EPO's legal framework may, under conditions closely mirroring the requirements of Article 23 GDPR, restrict the application of data subject rights (see paragraphs 33 et seq.). In the context of government access, the EDPB notes that the restriction contained in Circular No. 420 (h) may allow for an extensive interpretation, as it broadly refers scenarios of "*providing or receiving assistance to or from competent public authorities, including from the EPO's contracting States and international organisations*". While recognising that the scope of this provision is limited to the EPO staff, the EDPB invites the Commission to monitor its practical application.

4. IMPLEMENTATION AND MONITORING OF THE DRAFT DECISION

88. Concerning the monitoring and review of the adequacy decision, the EDPB notes that according to the case law of the CJEU, 'in the light of the fact that the level of protection ensured by a third country or an international organisation is liable to change, it is incumbent upon the Commission, after it has adopted an adequacy decision pursuant to Article 45 GDPR, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country or international organisation in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard'[46].

89. The EDPB considers that the oversight function - and in particular the exercise of investigative and corrective powers - as well as governmental access to data transferred from the EU to the EPO will deserve specific attention in the course of the next periodic reviews. Likewise, further attention should be given by the Commission during the monitoring of the adequacy decision to the evolution of the rules that supplement the DPR, such as the *"Decision of the President of the European Patent Office dated 12.07.2024 on the Enforceability of DPO Recommendations endorsed by the Data Protection Board in the framework of Data Protection Audits and Inspections",* the "*Data Protection Oversight -*

[44] While the EDPB acknowledges that all contracting states are parties to the ECHR and to Convention 108, the EDPB recalls that the ratification of such instruments may not by itself provide for an essentially equivalent level of protection, as this will depend, in particular, on their specific implementation in each country.
[45] EPO transmission and transfer of personal data, Explanatory Note, Version of January 2024, p. 6.
[46] CJEU, October 6, 2015, Judgment in case C-362/14, Maximillian Schrems v Data Protection Commissioner ("Schrems"), para 76. See also Draft Decision, Recital 105, and Article 3(5).

How the Data Protection Officer conducts DP Audits and DP Inspections", and the "*EPO transmission and transfer of personal data, Explanatory Note"* Version of January 2024.

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

91. Concerning the practical involvement of the EDPB and its representatives in the preparation and proceeding of the future periodic reviews, the EDPB reiterates that any relevant documentation, including correspondence, should be shared in writing with the EDPB sufficiently in advance of the reviews.

92. The EDPB welcomes that the Draft Decision foresees the participation of the EDPB in the meeting organised between the Commission and the EPO and dedicated to performing the review of the functioning of the adequacy decision.

For the European Data Protection Board

The Chair

(Anu Talus)