EUROPEAN
COMMISSION

Brussels, XXX
[…](2025) XXX draft

COMMISSION IMPLEMENTING DECISION

of XXX

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

(Text with EEA relevance)

COMMISSION IMPLEMENTING DECISION

of XXX

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

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

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

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

Whereas:

1. INTRODUCTION

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

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

(3) As specified in Article 45(2) of Regulation (EU) 2016/679, the adoption of an adequacy decision is to be based on a comprehensive analysis of the international organisation's legal regime, covering both the rules applicable to data importers and the limitations and safeguards as regards access to personal data by public authorities. In its assessment, the Commission must determine whether the international organisation in question guarantees a level of protection 'essentially

1 OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

2 See recital 101 of Regulation (EU) 2016/679.

equivalent' to that ensured within the Union[3]. The standard against which the 'essential equivalence' is assessed is that set by Union legislation, notably Regulation (EU) 2016/679, as well as the case law of the Court of Justice of the European Union[4]. The European Data Protection Board's (EDPB) 'adequacy referential' is also of significance in this regard to further clarify that standard and provide guidance[5].

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

(5) The Commission has analysed the legal framework and practice of the European Patent Organisation. Based on the findings set out in recitals 7 to 97, the Commission concludes that the European Patent Organisation (EPO) ensures an adequate level of protection for personal data transferred within the scope of Regulation (EU) 2016/679 from the Union to the EPO.

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

2. RULES APPLYING TO THE PROCESSING OF PERSONAL DATA

2.1. Organisation and tasks of the European Patent Organisation

(7) The European Patent Organisation is an intergovernmental organisation that was set up on 7 October 1977 on the basis of the European Patent Convention (EPC). The Organisation has its seat in Munich and has 39 contracting States, comprising all Member States of the Union, Iceland, Norway, and Liechtenstein, as well as Albania, North Macedonia, Monaco, San Marino, Serbia, Switzerland, Montenegro, the United Kingdom, and Türkiye[9].

(8) The Organisation has legal personality[10] and consists of two organs[11]: the European Patent Office (Office) and the Administrative Council. The EPO's main task is the

3 See recital 104 of Regulation (EU) 2016/679.
4 See Case C-311/18, Facebook Ireland and Schrems ('Schrems II') ECLI:EU:C:2020:559, paragraph 94.
5 European Data Protection Board, Adequacy Referential, WP 254 rev. 01, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
6 Case C-362/14, Schrems ('Schrems I'), ECLI:EU:C:2015:650, paragraph 73.
7 Schrems I, paragraph 74.
8 Schrems I, paragraph 75.
9 This reflects the number of contracting States as of February 2025.
10 Article 5(1) of the EPC.

granting of European patents[12] in accordance with the EPC, which is done by the Office under the supervision of the Administrative Council. The Administrative Council consists of representatives of the contracting States and it exercises legislative powers on behalf of the EPO. It is also responsible for policy issues and supervises the Office's activities[13]. The Office, which acts as the executive arm of the EPO, is headed by a President[14] who manages the Office (President) and is accountable to the Administrative Council[15]. The President, among other things, prepares and implements the Office's budget, appoints, and supervises the Office's staff, exercises disciplinary authority over staff, ensures the functioning of the Office including the adoption of internal administrative instructions and information to the public, and may submit to the Administrative Council any proposal for amending the Convention, general regulations, or decisions that fall within its competence[16]. The Office consists of different departments, including a Receiving Section, a Legal Division, Examining and Opposition Divisions, and the Boards of Appeal (an internal independent body before which decisions taken by the EPO in the context of the patent granting procedure can be appealed)[17].

(9) In the performance of its tasks, the EPO receives personal data from a number of different actors in the Union. On a continuous basis, European patent applications[18] are filed at EPO by patent applicants or transmitted to the EPO by national patent offices in Member States[19]. The EPO also receives and processes personal data in the context of the tasks entrusted to it under Regulation (EU) No 1257/2012 of the European Parliament and of the Council[20]. Those tasks include receiving and examining requests for unitary effect of European patents, collecting annual fees, and registering unitary effect[21]. In this context, the EPO also receives requests

---

11 Article 4(2) of the EPC.

12 In each of the contracting States for which it is granted, a European patent in principle has the effect of and is subject to the same conditions as national patent granted by that state (see Article 2(2) of the EPC).

13 Articles 26 and 33 of the EPC.

14 The President is appointed by the Administrative Council and represents the EPO externally (Article 5(3) of the EPC).

15 Article 10(1) of the EPC.

16 Article 10(2) of the EPC.

17 Members of the Boards of Appeal are appointed by the Administrative Council (on a proposal from the President) and operate independently (Articles 11(3) and 23 of the EPC).

18 This includes for example the name, address, nationality, and telephone number of applicants; name and address of inventors and patent representatives; name and financial information of the person making payments, etc. The EPO may obtain additional personal data if a third party opposes the granting of a patent, in which case additional information, such as third party observations, evidence and written statements may be shared with the EPO (see the Implementing Regulations to the EPC, for example R41(2), R143(1)(h), R92(2)(c), R19(1), R53(1), etc.). See also Article 9 of the President Decision on the patent-granting procedure.

19 A European patent application can be filed with the central industrial property office or other competent authority of a contracting State. After checking the application for security or other national requirements, the national authority forwards it to the EPO.

20 Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection (OJ L 361, 31.12.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/1257/oj).

21 Unitary Patents having unitary effect for all the participating Member States are registered centrally at the EPO, without the need for further administrative steps at national level (as is required for European patents).

about ongoing appeals before the Office's Board of Appeals[22] from the Unified Patent Court (UPC), which may include personal data necessary to identify the relevant case[23].

(10) Similarly, the EPO receives personal data contained in international patent applications when it acts under the Patent Cooperation Treaty (PCT), an international treaty that allows applicants to obtain patents with effects for all PCT contracting States[24]. The EPO acts as an International Search Authority under the PCT and in this capacity reviews patentability of inventions disclosed in international applications, which help applicants to determine whether or not to file an application for substantive examination at national/Union level[25].

(11) In addition, the EPO cooperates closely with national patent offices in all Member States in the context of a 'European Patent Network', and, in that context, exchanges personal data with them, for example when providing trainings courses and IT services to support and strengthen cooperation under the EPC. Similarly, it has concluded bilateral cooperation agreements with Member States that involve the exchange of personal data, for example in the context of the establishment of working groups, secondment and deployment of technical experts, etc. It also cooperates closely with the European Union Intellectual Property Office (EUIPO), for example by conducting joint trainings courses and awareness raising events, and seconding experts.

(12) Finally, the EPO has contracts with several service providers in the Union that act as a processor within the meaning of Article 4, point (8) of Regulation (EU) 2016/679 and transfer personal data to the EPO.

2.2. Applicable legal framework and data protection rules

(13) The primary legislation that governs the activities of the EPO is established by an international treaty, that is to say the European Patent Convention and, where the EPO acts under the Patent Cooperation Treaty, by the latter. At a second level of the hierarchy of norms applicable to the EPO are legal acts adopted by the Administrative Council or, as far as the PCT is concerned, by the PCT Assembly.

---

22 In December 2024, EPO adopted rule on an independent oversight mechanism for the processing of personal data by the Board of Appeal in their judicial capacity. Available at https://www.epo.org/en/about-us/transparency-portal?search_description=CA%2FD+19%2F24&op=&sort_by=most&items_per_page=10

23 The UPC has been established on the basis of the Agreement on a Unified Patent Court (OJ C 175, 20.6.2013, p. 1) and has exclusive jurisdiction *inter alia* with respect to European patents (subject to a transitional period) and European patents with unitary effect (for example as regards actions for actual or threatened infringements and related defences, actions for declaration of non-infringement, actions for provisional and protective measures and injunctions, actions for revocation and counterclaims for revocation). The UPC also has exclusive jurisdiction concerning decisions of the EPO in carrying out its tasks on Unitary Patent Protection.

24 For an overview of the PCT procedure, see the PCT Applicant's Guide – Introduction to the International Phase, available at https://www.wipo.int/pct/en/guide/index.html, in particular chapter 3, and the Guide for applicants: PCT procedure before the EPO (Euro-PCT Guide), 16th edition, 1 January 2023, available at https://www.epo.org/en/legal/guide-europct/2023/index.html. For the categories of personal data processed by the EPO in the context of proceedings under the PCT see, in particular, section 9(a), (d), (h), (i), (j), (l), (m), (n) and (p) of the Annex to the 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 (OJ EPO 2021, A98).

25 Also, here a patent application may have to be transferred from the central industrial property office or other competent authority of a PCT contracting State to the EPO.

Secondary legislation of the EPO includes Implementing Regulations to the EPC and so-called Service Regulations (which regulate aspects relating to the EPO's staff, including staff rights and obligations)[26]. The right to the protection of personal data is set out in Article 1B of the Service Regulations[27], which also contains some core provisions of the EPO's data protection framework, that is to say concerning the scope of application of the data protection framework, the protection of special categories of data and the exercise of rights by individuals. Article 2(1) and 32B of the Service Regulations establish independent oversight mechanisms (the Data Protection Officer (DPO) and the Data Protection Board (DPB)) to supervise compliance with the data protection rules.

(14) The same substantive requirements governing the protection of personal data apply to the Administrative Council and the Office, as well as all their departments. In particular, the processing of personal data by the Office is regulated by the Implementing Rules for Articles 1B and 32A of the Service Regulations for Permanent and Other Employees of the European Patent Office on the Protection of Personal Data (Data Protection Rules (DPR)), which have been adopted by the Administrative Council[28]. The processing of personal data by the Administrative Council is subject to the Administrative Council Data Protection Rules (AC DPR), which apply the DPR *mutatis mutandis*[29]. Where this Decision refers to the DPR, the references include the corresponding requirements that apply to the Administrative Council, its Secretariat and its committees. The structure and content of the DPR is closely aligned with the Union data protection framework[30]. In particular, it shares many commonalities with Regulation (EU) 2018/1725 of the

---

26 Article 33 of the EPC.

27 See in particular Article 1B(1) of the Service Regulations, which provides that 'the Office endeavours to ensure respect for the fundamental rights to privacy and to the protection of personal data of all individuals whose data are processed by the Office, and to guarantee accountability in this regard.' See also Article 1(1) of the DPR, which explains that the DPR provide the legal framework necessary to ensure that 'the fundamental rights of natural persons to privacy and to the protection of their personal data processed by the Office are observed'.

28 Data Protection Rules (from p. 495), available at https://report-archive.epo.org/files/babylon/service_regulations_en.pdf. The DPR also applies to the Office's Boards of Appeal, with the exception of the redress procedure before the Data Protection Board, which does not apply to the processing of personal data by the Boards in their judicial capacity (Article 2(6) of the DPR). For those activities, the DPR requires the Boards to establish a separate independent review mechanism.

29 Administrative Council Data Protection Rules, available at https://link.epo.org/ac-document/CA/D%202/23%20-%20En.pdf. The only aspect on which the Administrative Council Data Protection Rules differ from the DPR concerns adaptations to the specific set-up of the Administrative Council, that is to say by replacing references to the President with references to the Chair of the Administrative Council. In addition, separate rules - the Select Committee Data Protection Rules (SC DPR) - have been adopted for the so-called Select Committee of the Administrative Council. This Committee is composed of EPO's contracting States and user organisations and has been established by Article 9(2) of Regulation (EU) No 1257/2012 and Article 145 EPC to supervise the Office's activities in the context of the unitary patent procedure. The Select Committee Data Protection Rules apply the Administrative Council Data Protection Rules (which in turn apply the DPR) to the processing of personal data by the Select Committee (see https://link.epo.org/web/about-us/governance/SC_D_1_23_en.pdf). Also here, the Select Committee Data Protection Rules only differ from the rules for the Administrative Council and Office by referring to the Chair of the Committee (instead of the Chair of the Council or the President).

30 EPO's Data Protection Rules: https://www.epo.org/en/about-us/office/data-protection-and-privacy

European Parliament and of the Council[31] which lays down data protection requirements for the Union institutions and bodies and is thus well suited to the specific structure and features of international organisations, while closely mirroring Regulation (EU) 2016/679.

(15) As regards data processing by the Office, further legally binding instruments have been issued by the President, such as circulars, decisions, and internal administrative instructions[32]. In particular, the DPR is complemented by Decision of 13 December 2021 of the President concerning the processing of personal data in patent-grant and related proceedings (PGP Decision)[33]; Decision of 7 December 2022 concerning the processing of personal data in proceedings related to European patents with unitary effect (UP Decision)[34]; Decision of 17 November 2022 concerning countries and entities considered to ensure adequate protection of personal data[35]; Decision of 2 May 2024 identifying the operational units of the Office acting as delegated controllers[36]; and Circular No. 420 Implementing Article 25 of the DPR on restrictions to data subject rights (Circular 420)[37]. Specifically for the processing of data in the context of patent granting proceedings, it is important to note that requirements for the processing of personal data provided for directly in the EPC and PCT prevail over the DPR. The interplay between the EPC and PCT on the one hand and the DPR on the other is clarified in the PGP Decision[38] and the UP Decision. The specific data protection requirements following directly from the EPC and PCT are assessed in recitals 55 to 59. The DPR and its complementary instruments are legally binding and enforceable and can be invoked by individuals before independent redress mechanisms, as described in recitals 88 to 95.

(16) The rules provided for in the legal instruments mentioned in recital 15 are further operationalised in instruments issued by the Data Protection Officer (see recitals 82

31 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

32 Article 10 EPC. See also Article 1(2)(a) of the DPR.

33 https://www.epo.org/en/legal/official-journal/2021/12/a98.html. A similar decision has been adopted as regards the processing of data in appeal proceedings before the Boards of Appeal by the President of the Boards of Appeal, that is to say the Decision dated 14 July 2023 concerning the processing of personal data in appeal proceedings before the Boards of Appeal, available here https://www.epo.org/en/legal/official-journal/2023/07/a73.html.

34 Decision of 7 December 2022 concerning the processing of personal data in proceedings related to European patents with unitary effect, available at https://www.epo.org/en/legal/official-journal/2022/12/a112.html.

35 https://epo.org/en/legal/official-journal/2022/12/a111.html. As amended by Decision of 11 May 2023, (OJ EPO 2023, A57) available at https://www.epo.org/en/legal/official-journal/2023/06/a57.html.

36 https://link.epo.org/web/en-decision-of-the-president-on-delegated-controllers.pdf. This Decision is updated at least annually.

37 Circular 420 Implementing Article 25 of the Data Protection Rules, available at https://link.epo.org/web/circular_420_en.pdf.

38 As regards the processing of personal data by the Boards of Appeal in appeal proceedings, this interplay is clarified in the Decision of the President of the Boards of Appeal concerning the processing of personal data in appeal proceedings before the Boards of Appeal.

to 87)[39], which apply to the Administrative Council and the Office, as well as all of their departments[40].

2.3. Material and personal scope of the Data Protection Rules

(17) Pursuant to the DPR and the Service Regulations[41], all employees of the EPO are required to comply with the DPR when processing personal data. The material and personal scope of application of the DPR is determined by the terms 'personal data,' 'processing,' 'controller', 'delegated controller' and 'processor' therein defined.

2.3.1. Definition of personal data and processing

(18) The definitions of 'personal data' and 'processing' in the DPR are identical to the ones in Regulation (EU) 2016/679[42]. The DPR applies to any processing of personal data by the EPO, regardless of whether such processing concerns personal data of its own employees or data of other individuals[43]. Data that has undergone pseudonymisation[44] is also considered personal data, whereas data of deceased persons or legal persons, or anonymous information[45] is not treated as personal data under the DPR[46].

(19) The DPR applies to the processing of personal data by the EPO wholly or partly by automated means and to processing other than by automated means of personal data which form or are intended to form part of a filing system[47].

2.3.2. Controller, delegated controller, and processor

---

39 See for example the reference to operational documents issued by the DPO in Article 1(2)(c) DPR, which have been approved by the President and have thereby become binding.

40 See Article 1(6) and Article 12(5) of the Administrative Council DPR.

41 Article 2(2) of the DPR and Article 1 of the Service Regulations.

42 Article 3(1)(a) and (b) of the DPR and Article 4(1) and (2) of the GDPR.

43 Article 1B(2) of the Service Regulations and Article 2(2) and (3) of the DPR. See also the definition of 'data subject' (Article 3(1)(w) of the DPR), that is to say 'any identified or identifiable natural person, irrespective of whether that person is an employee of the Office or not'. To determine whether an individual is identifiable, account must be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly.

44 That is to say 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person', see Article 3(1)(e) of the DPR.

45 That is to say 'information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable', see Article 3(1)(r) of the DPR. Pursuant to Article 13(1) of the DPR, the controller is not required to maintain, acquire or process additional information to identify an individual for the sole purpose of complying with the DPR, where the purposes for which the data are processed do not or no longer require identification of an individual.

46 Article 2(4) of the DPR. With respect to the processing of personal data for archiving purposes (in the legitimate exercise of the EPO's official authority), scientific or historical research purposes or statistical purposes, the DPR requires that technical and organisational measures are in place, inter alia to ensure respect for the principle of data minimisation and, where the purpose of processing can be achieved in that manner, process data in a way that no longer permits identification of the individual (Article 14 of the DPR).

47 Article 1B(3) of the Service Regulations and Article 2(1) of the DPR. 'Filing system' is defined as 'any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis', see Article 3(1)(f) of the DPR.

(20) The DPR defines a 'controller' as an 'an entity, namely the European Patent Office, which, alone or jointly with others, determines the purposes and means of the processing of personal data'[48]. In principle, the President acts as a controller for the data processing operations carried out by the Office[49]. The same applies to the Administrative Council (where the Chair acts as controller), the Boards of Appeal acting in its judicial capacity (where its President acts as controller[50]) and the Select Committee (where the Chair acts as controller[51]). The controller can delegate this power to operational units, represented by a manager at senior level[52]. In such cases, operational units act as 'delegated controllers'[53] that define the purpose (for example reason, rationale and business needs), the means of a processing operation, and ensure that all processing operations involving personal data comply with the rules of the DPR[54]. The DPR also provides for a scenario of 'joint controllership,' where a controller determines the purpose and means of processing together with one or more controllers outside the EPO[55].

(21) The definition of 'processor' in the DPR is identical to the one in Article 4(8) of Regulation (EU) 2016/679, that is to say a natural or legal person, public authority, agency, or any other entity which processes personal data on behalf of the controller[56]. The controller is only allowed to use processors providing sufficient guarantees that appropriate technical and organisational measures will be implemented to ensure that the processing meets the requirements of DPR[57]. The relationship between the controller and a processor must be governed by a contract or legal act that is binding on the processor and, among other things, sets out the subject-matter, duration, nature and purpose of the processing[58]. The processor is only allowed to process the data on documented instructions of the controller. The processor is required to assist the controller with fulfilling its obligations under the DPR The processor is prohibited from engaging sub-processors without the prior authorisation of the controller[59]. A standard data processing agreement is available

48 Article 3(1)(g) of the DPR. When using the term 'controller' in this Decision, this refers either to the EPO itself or to delegated controllers.

49 Article 10(2) of the EPC and article 28(1) of the DPR.

50 Article 28(2) of the DPR. This follows specifically from a delegation of power from the Office's President, see https://www.epo.org/en/legal/official-journal/2021/etc/se1/p175.html. For other activities (where the Boards do not act in their judicial capacity), the Boards' President acts as delegated controller for the President of the Office.

51 See Article 1(4)(5) of the AC DPR and Article 13a(2) of the Rules of Procedure of the Select Committee.

52 Article 28(3) of the DPR.

53 See Article 3(1)(h) of the DPR. The person representing the operational unit must be a manager at senior level, normally at least a principal director. The list of delegated controllers is made public (see for example, https://link.epo.org/web/decision_of_the_president_on_delegated_controllers_en.pdf and https://link.epo.org/web/decision_of_the_president_of_the_boards_of_appeal_appointing_a_delegated_controller_en.pdf) and is updated regularly.

54 When this Decision refers to a 'controller', this includes relevant delegated controllers.

55 In this case, Article 29 of the DPR requires the (delegated) controller to determine, in a transparent manner, the respective responsibilities of both parties for compliance with their data protection obligations, in particular as regards the exercise of rights of individuals and transparency obligations.

56 Article 3(1)(j) of the DPR.

57 Article 30(1) of the DPR.

58 Article 30(3) of the DPR.

59 Article 30(2)-(3) of the DPR. A processor engaging a sub-processor is (contractually) required to impose the same data protection obligations on the sub-processor as the ones provided in the contract between the controller and processor (Article 30(4) of the DPR).

to delegated controllers[60]. Moreover, if a processor is located in a third country, any sharing of personal data with that processor must also comply with the DPR's requirements for international transfers, as described in recitals 67 to 72 of this Decision[61].

2.4. Safeguards, rights and obligations

2.4.1. Lawfulness and fairness of processing

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

(23) Those general principles are laid down in Article 4(2)(a) DPR in a way that can be considered identical to Article 5(a) of Regulation (EU) 2016/679.

(24) The principle of lawfulness is further developed in Article 5 DPR, which lists the legal bases on which personal data may be processed. Those legal bases are (a) the necessity to carry out a task in the exercise of the official activities of the EPO[62] or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning[63]; (b) the necessity to comply with a legal obligation to which the controller is subject (for example to publish information mentioned in a patent application in the European Patent Register)[64]; (c) the necessity to perform a contract to which the data subject is a party or to take steps at request of the data subject prior to entering a contract; (d) the data subject's consent; or (e) the necessity to protect the vital interests of the data subject or another natural person.

(25) Consent is defined in the DPR in the same way as in Regulation (EU) 2016/679, that is to say 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to processing of personal data relating to him or her'[65]. It is for the controller to demonstrate that the data subject has consented[66]. When assessing whether consent is freely given, account should be

---

60 Annex E of the general conditions of contract for the EPO, https://link.epo.org/web/general_conditions_of_contract_en.pdf.

61 Article 8(1), (2) and (5), in conjunction with Article 9(1) of the DPR.

62 This refers to tasks carried out under the EPC and the PCT or rules adopted on that basis (for example the Service Regulations) that are necessary to perform the EPO's tasks in the patent granting procedure. See also paragraph 5(1) of the Annex to the PGP Decision and relevant provisions of the EPC, such as its Part IV and V. For the performance of the EPO's tasks in the context of the patent granting procedure, the EPO processes personal data for processing applications and patents; conducting opposition proceedings; communicating with the parties to the proceedings (and where applicable, third parties); maintaining the European Patent Register; drawing up reports and statistics and exchanging data with contracting States and the World Intellectual Property Organization (paragraph 6 of the Annex to the PGP Decision).

63 This captures the tasks assigned to the Office's President to ensure the effective functioning and management of the Office. See for example Article 10 of the EPC, which describes the tasks of the President as regards staff, (access to) buildings and equipment management. This approach is in line with Article 5(1)(a) and recital 22 of Regulation (EU) 2018/1725. Similarly, this refers to the Administrative Council's tasks under the EPC, for example to establish rules on pensions and financial regulations, see Article 33 EPC, Rules 9(2), 12(c) and 122(4) of the Implementing Regulations to the EPC. As regards the Select Committee, this refers to the supervisory tasks under Article 145 of the EPC. Finally, for the Boards of Appeal, this for instance refers to its responsibility for examining appeals against decisions of other parts of the Office, see Article 21(1) of the EPC.

64 See for example Rule 20 Implementing Regulations to the EPC.

65 Article 3(1)(m) of the DPR. See also Article 7(2) of the DPR.

66 Article 7(1) of the DPR

taken of whether the performance of a contract is conditional on consent to the processing of data that is not necessary for the performance of that contract[67]. Consent cannot be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment[68]. Moreover, for consent to be informed, the DPR requires the data subject to be aware at least of the identity of the controller and the purposes of the processing for which personal data are intended[69]. Finally, a data subject has the right to withdraw consent at any time[70].

2.4.2. Processing of special categories of data

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

(27) The DPR contains specific rules as regards the processing of special categories of personal data[71], which are defined in the same way as under Regulation (EU) 2016/679, that is to say 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic data[72] or biometric data[73] for the purpose of uniquely identifying a natural person and of data concerning health[74] or data concerning a natural person's sex life or sexual orientation'[75]. Pursuant to the DPR, the processing of special categories of data is in principle prohibited unless a specific exception applies[76].

(28) The specific exceptions listed in Article 11(2) DPR are similar to those in Article 9(2) and (3) of Regulation (EU) 2016/679, with a few adaptions to the legal framework in which the EPO operates. The processing of special categories of personal data is only permitted in specific and limited circumstances[77], that is to say

---

67 Article 7(1), (5), (6) and (7) of the DPR.

68 Article 7(4) of the DPR.

69 Article 7(4) of the DPR.

70 Article 7(5) of the DPR.

71 See for example Article 11 of the DPR.

72 Defined as 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from that natural person', see Article 3(1)(o) of the DPR.

73 Defined as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data', see Article 3(1)(p) of the DPR.

74 That is to say personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status, see Article 3(1)(q) of the DPR.

75 Article 11(1) DPR.

76 Article 11(1) and (2) of the DPR.

77 The DPR also allow the processing of special categories of data in specific scenario's that mostly concern the EPO's staff and are therefore less relevant for data transferred on the basis of this decision. In particular, special categories of data may be processed where authorised by a legally binding provision that applies to the European Patent Organisation (for example the EPC and instruments adopted by the Administrative Council and the President, see Article 3(1)(x) of the DPR) that provides for appropriate safeguards for the fundamental rights and interests of the data subject (Article 111(2)(b) of the DPR) and is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security law. Similarly, the processing may take place where necessary for reasons of public interest in the area of public health (such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare, on the basis of national law which provides for suitable and specific

where (1) the data subject has given explicit consent; (2) the processing is necessary to protect the vital interests of an individual (where the data subject is physically or legally incapable of giving explicit consent); (3) the personal data has been manifestly made public by the data subject; (4) the processing is necessary for a specific purpose relating to the exercise of the official activities of the EPO or in the exercise of legitimate authority vested in the controller[78]; or (5) the processing is necessary for the establishment, exercise or defence of legal claims.

(29) In addition to the special categories of personal data referred to in recital 27, the DPR also requires specific protections for the processing of personal data relating to criminal convictions and offences, that is to say by only allowing such processing after prior consultation of the DPB or where the processing is required by a legally binding instrument that provides for appropriate safeguards for the rights and freedoms of individuals[79].

2.4.3. Purpose limitation

(30) Personal data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of processing.

(31) That principle is ensured in Article 4(2)(b) DPR, pursuant to which personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with these purposes'.

(32) Similar to Regulation (EU) 2016/679, the DPR allows further processing (regardless of the compatibility of the purpose of the further processing with the original one) on the basis of the data subject's explicit consent or on the basis of applicable legal provisions of the EPO[80]. In the latter case, the DPR requires that the processing must be a necessary and proportionate measure to safeguard a general public interest objective[81].

(33) Where further processing is not based on those two grounds, the DPR provides for the factors to be taken into account when assessing the compatibility of the purpose for further processing with the purpose for which the personal data were originally

---

measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy, see Article 11(2)(g) of the DPR). Finally, processing may be required for preventive or occupational medicine, the assessment of an employee's working capacity, medical diagnosis, the provision of health or social care or treatment, the management of health or social care systems and services or medical examinations and opinions, where those data are processed by a health professional subject to the obligation of professional secrecy or by another person subject to an equivalent obligation of secrecy (Article 11(3) of the DPR).

78 For example, in the context of appeals against granted patent, sensitive data could be included in witness statements or submitted evidence. Processing under this provision may also take place if substantially necessary for the management and functioning of the Office and for obligations arising from the EPO's obligation of co-operation with the contracting States (for example the need to process health information of staff or visitors in accordance with requirements imposed by public health authorities of the EPO's host State). In any event, the legal instrument on which the processing is based must be proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 11(2)(f) of the DPR).

79 Article 12 of the DPR. A possible scenario where such data would be processed includes disciplinary proceedings concerning patent attorneys before the EPO's Disciplinary Board (see for example para. A.7 Annex to the PGP Decision).

80 Article 6 (2) of the DPR.

81 For example, the Organisation's security; the prevention, investigation, detection, and prosecution of criminal offences; the rights and freedoms of others, etc. (see Article 25(1) of the DPR).

collected[82]. This approach and the factors listed in the DPC are identical to those set out in Article 6(4) of Regulation (EU) 2016/679 and Article 6 of Regulation (EU) 2018/1725[83].

2.4.4. Data accuracy and minimisation, storage limitation and data security

(34) Personal data should be accurate and, where necessary, kept up to date. It should also be adequate, relevant and not excessive in relation to the purposes for which it is processed, and in principle be kept for no longer than is necessary for the purposes for which the personal data is processed.

(35) Those principles are laid down in Article 4(2)(c), (d) and (e) of the DPR in the same way as in Regulation (EU) 2016/679.

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

(37) Data security is enshrined in the legal framework of the EPO through the principle of integrity and confidentiality laid down in Article 4(2)(f) and Article 33 of the DPR, in an almost identical way as in Regulation (EU) 2016/679. In particular, the DPR requires that a level of security appropriate to the risk is ensured through appropriate technical and organisational measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the varying likelihood and severity of any risks for the rights and freedoms of individuals.

(38) In addition, the DPR contains specific requirements on the handling and notification of a data breach[84]. First, the controller is required to notify the DPO of a data breach without undue delay (and, where feasible, no later than 72 hours after having become aware of it), unless the breach is unlikely to result in a risk to the rights and freedoms of individuals[85]. A processor is similarly required to notify the controller of a breach without undue delay[86]. The notification must, in particular, describe the nature of the breach, its likely consequences and the measures taken or proposed to be taken to address the breach[87]. Where a data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must also communicate the personal data breach to the data subject without delay[88]. The communication to the data subject must describe the nature of the personal data breach in clear and plain language[89] and is not required if the controller has taken

---

82 Article 6(3) of the DPR.

83 In particular, any link between the purpose of collection and the purpose of the intended further processing; the context in which the data was collected; the nature of the data; and the possible consequences of the further processing for individuals, see Article 6(3) of the DPR.

84 'Data breach' is defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed', see Article 3(1)(n) of the DPR.

85 Article 34(1) of the DPR.

86 Article 34(2) of the DPR.

87 Article 34(1) and 3 of the DPR.

88 Article 34(6) of the DPR.

89 Article 34(6) of the DPR.

subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer to materialise[90].

2.4.5. Transparency

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

(40) In accordance with the DPR, the controller is required to, at the time when obtaining personal data, provide individuals with information, in particular, on its identity and contact details (as well as the contact details of the DPO), the purpose of processing and the legal basis thereof, the recipients or categories of recipients, the fact that it intends to transfer the data outside of the EPO, as well as applicable rights and the possibility to obtain redress[91]. The same applies when personal data is processed for a purpose other than that for which the data was collected[92]. Both obligations only apply in as far as the concerned individual does not yet have the information[93].

(41) The same information must be provided to the data subjects when personal data is not collected directly from them, together with additional information on the source of the personal data and the categories of data concerned[94]. Such information must be provided within a reasonable time after obtaining the data (but at the latest within one month), having regard to the specific circumstances in which the data is processed[95]. In case that personal data are to be used for communication with the data subject, the same information should be provided at the latest at the time of the first communication with the individual.[96] The information referred to in recital 40 must also be provided prior to any further processing or, if a disclosure to another recipient is envisaged, at the latest when personal data are disclosed to a third party[97]. That obligation does not apply in a number of cases, namely where a data subject already has the information concerned; where that information must remain confidential because of an obligation of professional secrecy regulated on the basis of the EPC and/or other legal provisions applicable to the EPO[98]; where the provision of that information proves impossible or would involve disproportionate effort, in particular for processing for archiving, scientific or historical research, or statistics, in so far as it would render impossible or seriously impair the achievement of the objectives of the processing; or where obtaining or disclosure of that information is expressly laid down in the EPC or other applicable legal

90 Article 34(8) of the DPR.
91 Article 16(1)-(2) of the DPR.
92 Article 16(3) of the DPR.
93 Article 16(4) of the DPR.
94 Article 17(1) and (2) of the DPR.
95 Article 17(3)(a) of the DPR.
96 Article 17(3)(b) of the DPR.
97 Article 17(3)(c) and (4) of the DPR. A third party is defined in Article 3(1)(l) of the DPR as any natural or legal person, public authority, agency, or body other than the data subject, the controller, the processor, and the persons who, under the direct authority of the controller or the processor, are authorised to process personal data.
98 Article 17(4) of the DPR. Such confidentiality requirements for instance apply in the context of the processing of personal data of staff by the EPO's medical service (in which case the relevant medical practitioners may be under an obligation of professional secrecy, see for example Paragraph A(2) and Implementing Rules for Articles 83a, 84 and 84a of the Service Regulations, para E) or in the context of recruitment proceedings (section 6 of Annex II – Competition Procedures for Posts for which the President is the Appointing Authority).

provisions that provide appropriate measures to protect the data subject's legitimate interests[99].

2.4.6. Individual rights

(42) Data subjects should have certain rights which can be enforced against the controller or processor, in particular the right of access to data, the right to rectification, the right to object to processing and the right to have data erased. At the same time, such rights may be subject to restrictions, insofar as these restrictions are necessary and proportionate to safeguard important objectives of general public interest.

2.4.6.1. Rights provided by the DPR

(43) The need to facilitate the exercise of individual rights is laid down in Article 1B(4) of the Service Regulations. To further implement this requirement, the DPR provides individuals with the same rights as those laid down in Regulation (EU) 2016/679, namely a right of access (Article 18 of the DPR), a right to rectification (Article 19 of the DPR), a right to erasure (Article 20 of the DPR), a right to restriction of processing (Article 21 of the DPR), a right to data portability (Article 22 of the DPR), a right to object (Article 23 of the DPR) and a right not to be subject to automated decision-making (Article 24 of the DPR).

(44) The DPR also lays down general provisions for the handling of requests for the exercise of rights from individuals, requiring the controller to communicate with data subjects using clear and plain language, in a concise, transparent, intelligible, and easily accessible form (in writing or by other means)[100]. The controller must provide individuals with information on the measures taken in response to a request without undue delay and in any event within one month of the receipt of the request (which may be extended with two further months where necessary in view of the complexity and number of requests)[101]. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request[102]. When the controller does not act upon a request, it must inform the individual thereof and provide information on the possibility to seek redress[103].

(45) Firstly, as regards the right of access, the DPR provides individuals with the right to obtain from the EPO confirmation as to whether or not personal data concerning them are processed and, if so, to access the personal data easily[104] and at reasonable intervals[105]. In addition, individuals have the right to obtain information, in

---

99 That is to say where the EPC or legal instruments adopted on its bases specifically regulate the information to be disclosed to individuals or the public, see in more detail section 1.4.6.7 below.

100 Article 15(1) of the DPR.

101 Article 15(2) of the DPR.

102 Article 15(4) of the DPR. In addition, Article 13(2) of the DPR makes clear that, if the controller is able to demonstrate that it is not in a position to identify the data subject, the provisions on individual rights do not apply (unless the data subject provides additional information enabling their identification).

103 Article 15(3) of the DPR.

104 In particular, the controller must provide a copy in an intelligible form of the data undergoing processing and of all available information (of any kind, regardless of its nature (objective or subjective), content (including any type of activity undertaken), or format (paper file, computer records, emails), see Article 18(3) of the DPR. At the same time, the right to obtain a copy of the data may not adversely affect the rights and freedoms of others (Article 18(5) of the DPR).

105 Article 18(1) of the DPR.

particular, on the purpose of processing, the categories of data concerned, the recipients with whom data is shared, and the envisaged period for which data will be stored[106].

(46) Secondly, the DPR provides that the right to rectification provided for under the DPR allows individuals to obtain the rectification of inaccurate data or the completion of incomplete data (for example by means of providing a supplementary statement)[107]. Once rectification takes place, the controller is required to communicate it to each recipient to whom the personal data have been disclosed[108]. Pursuant to the DPR, the right to rectification applies to objective and factual data and not to subjective statements[109], although in this case individuals are allowed to complement existing data with a second opinion or counter-expertise or provide comments[110].

(47) Thirdly, the DPR also provides individuals with a right to erasure[111], in particular if (a) personal data are no longer necessary for the purpose for which they are processed; (b) the data subject withdraws consent and there is no other legal basis for the processing; (c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing; (d) the data was processed unlawfully; (e) or the data has to be erased to comply with a legal obligation that applies to the controller[112]. The controller must communicate any erasure to each recipient with whom the data has been shared unless this proves impossible or involves disproportionate effort[113]. Similarly, if the controller made the personal data public, it must take reasonable steps to inform other controllers that are processing it that erasure has been requested by the individual[114]. The right to erasure does not apply to the following scenarios, to the extent that the processing of the data is necessary, (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation of the EPO or an obligation deriving from the EPO's duty to cooperate with its contracting States[115] or for the exercise of official authority vested in the EPO[116]; (c) for reasons of co-operation

106 Article 18(2)-(3) of the DPR.

107 Article 19(1) of the DPR.

108 Article 19(3) of the DPR. If the data subject requests it, the controller has to inform about those recipients.

109 This interpretation was adopted in line with the EDPS Guidelines on the Rights of Individuals with regard to the Processing of Personal Data. https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf See in particular, p.18, guidance on the right to rectification referring to 'objective and factual data' and 'subjective statements'.

110 Article 19(2) of the DPR.

111 Erasure of data is defined as the 'obliteration of stored data in such a way that reconstruction is not possible' (Article 3(1)(v) of the DPR). The reference to 'stored data' covers all data collected and held by the controller (and any third parties on behalf of the controller).

112 Article 20(1) of the DPR.

113 Article 20(4) of the DPR.

114 Article 20(2) of the DPR.

115 Pursuant to Article 20 of the EPO Protocol on Privileges and Immunities, EPO may be required to provide personal data to its contracting States in the context of administrative or legal proceedings, for example for the calculation and transfer of pension rights of staff, for tax investigations, or in the context of civil trials concerning EPO's staff.

116 This refers to situations where the EPO is required under the EPC, PCT or legal instruments adopted on that basis to process personal data in relation to the patent granting procedure (for example maintaining information in the European Patent Register and the European Patent Bulletin under Article 127 and 129 of the EPC).

with the contracting States in the area of public health[117]; (d) for archiving, scientific or historical research and statistical purposes (in so far as erasure would likely render impossible or seriously impair the achievement of the objectives of the processing); or (e) for the establishment, exercise or defence of a legal claims[118].

(48) Fourthly, Article 21 of the DPR provides a right to restriction of processing, that is to say the marking of personal data with the aim of limiting their processing in the future (including programming measures to permanently prevent access to such data)[119]. That right can, in particular, be invoked where the accuracy of personal data is contested by the individual (for a period required by the controller to verify the accuracy) or where the processing is unlawful, but the individual opposes to the erasure of the data[120]. Where processing is restricted, personal data may, with the exception of storage, only be processed with the individual's explicit consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of others or for the performance of a task carried out in the exercise of the official activities of the EPO (that is to say a task which is necessary for the administrative and technical work that the EPO is required to perform in accordance with the EPC)[121].

(49) Fifthly, a right to object is set out in Article 1B(4) of the Service Regulations and Article 23 of the DPR. In particular, individuals have the right to object at any time to processing of personal data carried out for the performance of a task in the exercise of the official activities of the EPO or in the legitimate exercise of the official authority vested in the controller[122]. Individuals must be informed of the existence of such right in a clear manner and at the latest at the time of the first communication with them[123]. In case an individual object to the processing of personal data, the DPR requires the controller to cease the processing unless the controller is able to demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise or defence of legal claims[124].

(50) Sixthly, the DPR establishes a right to data portability, providing individuals with the possibility to receive their personal data in a structured, commonly used and machine-readable format, and to transmit that data to another controller[125]. Such right applies where the processing is carried out by automated means and takes

---

117 Processing of health data for reasons of public interest in the area of public health must be in accordance with Article 11(2)(g) of the DPR.

118 Article 20(3) of the DPR.

119 Article 3(1)(c) of the DPR.

120 Article 21(1) of the DPR.

121 Article 21(2) of the DPR.

122 Where the EPO is legally required to process personal data in the context of the patent granting procedure, that is to say under the EPC and the PCT, individuals cannot object to the processing, see paragraph 28 of the Annex to the PGP Decision. Where personal data are processed for scientific or historical research purposes or statistical purposes, data subjects have the right to object, on grounds relating to their particular situation, to processing of personal data unless the processing is necessary for the performance of a task carried out in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning (Article 23(4) of the DPR).

123 Article 23(2) of the DPR.

124 Article 23(1) of the DPR.

125 Article 22(1) of the DPR.

place on the basis of the consent of the individual, or for the performance of a contract with or in the interest of the individual[126].

(51) Finally, pursuant to the DPR, individuals have a right not to be subject to automated decision-making, that is to say a decision based solely on automated processing, including profiling, which produces legal effects concerning or similarly significantly affecting him or her[127]. The DPR sets out that automated decision-making may take place where it is based on the data subject's explicit consent or if it is necessary for entering into, or the performance of, a contract with the individual, in which case the controller must implement suitable safeguards, such as by providing the right to obtain human intervention, express the individuals' point of view, and to contest the decision[128]. Automated decision-making may also be authorised by a legal act if that act lays down suitable measures to safeguard the rights of individuals[129]. If the controller engages in automated decision-making, including profiling, it must proactively inform the individual thereof as part of its transparency obligations and provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject[130]. The same information must be provided upon request[131].

2.4.6.2. Restrictions to individual rights

(52) Similar to Article 23 of Regulation (EU) 2016/679 and Article 25 of Regulation (EU) 2018/1725, Article 25 DPR provides that specific legal provisions in the EPO's legal framework may restrict the application of the rights referred to in recitals 43 to 51[132] (that is to say limit their application temporarily)[133], when such a restriction respects the essence of fundamental rights[134] and freedoms and is a necessary and proportionate measure in a democratic society to safeguard specific objectives[135]. Furthermore, a restriction must be provided in 'clear and precise'

126 Since the processing of personal data in the context of the patent granting procedure is not based on either of those grounds, the right to data portability does not apply in such context, see paragraphs 29-30 Annex to the PGP Decision.

127 Article 24(1) of the DPR. Profiling is defined in Article 3(1)(d) of the DPR as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

128 Article 24(3) of the DPR.

129 Article 24(2)(b) of the DPR.

130 See Article 16(2)(f) and 17(2)(f) of the DPR.

131 Article 18(1)(h) of the DPR.

132 With the exception of the right to object, for which Circular 420 does not provide for any restrictions, see Article 3(3). In addition, pursuant to Article 9 of Circular 420, the EPO may restrict the communication of a data breach to an individual.

133 See the definition of restrictions in Article 2 of Circular 420.

134 Restrictions that are so extensive and intrusive that, in effect, deprive a fundamental right of its basic substance and prevent the individual from exercising it, cannot be justified, see Article 4(3) of Circular 420.

135 That is to say the EPO's security, public security or defence of the contracting States; the prevention, investigation, detection and prosecution of criminal offences or the enforcement of criminal penalties, including the safeguarding against and the prevention of threats to public security; other substantial interests of the EPO pertaining to its core mission, or in reason of obligations arising from the duty of co-operation with the contracting States, including monetary, budgetary and taxation matters, public health and social security; the internal security of the Office, including of its electronic communications networks; the protection of judicial and quasi-judicial independence and judicial and quasi-judicial

provisions that are intended to produce legal effects vis-à-vis data subjects and that must be adopted at least at the level of the President[136]. Such provisions must, in particular, lay down the purpose of processing, the scope of the restriction, the safeguards to prevent abuse and the storage periods and applicable safeguards[137].

(53) Currently, the only legal instrument that provides for restrictions to individual rights is Circular 420 (a legally binding instrument adopted by the President). It clarifies how and under which conditions restrictions can be applied by the controller and lays down, in an exhaustive way, the specific scenarios in which rights can be restricted and for which objectives[138]. In particular, it provides that the EPO may restrict individual rights for certain specific objectives: (a and b) when conducting investigative or disciplinary proceedings in relation to its staff[139]; (c) in the context of internal dispute settlement or the establishment, exercise or defence of legal claims, including arbitration, to preserve confidential information and documents obtained from the parties, interveners or other legitimate sources; (d) when processing health data in medical procedures and files, but only to protect the rights of individuals[140]; (e and f) when conducting internal audits and inspections (the latter are conducted by the DPO); (g) for the purposes of IT incident management and physical security incident reports; and (h) when providing or receiving assistance to or from competent public authorities, including from the EPO's contracting States and international organisations, or when co-operating with them on activities defined in relevant service level agreements, memoranda of understanding and co-operation agreements, either at their request or on the Office's own initiative[141].

(54) Whether or not a restriction can be applied in a specific case is to be determined by the controller in individual cases in light of the relevant circumstances[142]. In deciding whether or not to apply a restriction, the controller first must assess the necessity and proportionality thereof in the specific case, with the involvement of

---

proceedings; the prevention, investigation, detection and sanction of breaches of ethics for regulated professions; a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority; the protection of the data subject or the rights and freedoms of others and the enforcement of civil law claims (Article 25(1) of the DPR).

136 Article 25(3) of the DPR.

137 Article 25(2) of the DPR.

138 Article 1 of Circular 420.

139 Article 4(1)(a)-(b) of Circular 420.

140 This only concerns the processing of health data of EPO staff (and is this not directly relevant for the purposes of an adequacy finding that concerns the processing of data transferred from a controller or processor subject to the GDPR). Article 8 of Circular 420 further clarifies how restrictions to the right of access to medical data/files may be applied. In particular, it specifies that such a restriction may only be applied to the right to directly access their personal medical data and/or files of a psychological or psychiatric nature which are processed by the Office but only if access to those data is likely to adversely affect and pose an immediate danger to the life and health of the data subject or others.

141 Article 4(1) of Circular 420. This provision generally only concerns personal data of EPO staff. It refers to cases where the EPO is required to cooperate with national authorities of the contracting States under Article 131 of the EPC (which regulates cooperation between the EPO and national courts of the contracting States in investigations/proceedings relating to patent granting) and under Article 20(1) of its Protocol on Privileges and Immunities (see also paragraph 95). This may for example be the case where EPO staff is requested to testify in a national court of a contracting State in the context of national criminal proceedings, or EPO is asked to provide information on salary of its staff in civil (family law) proceedings, etc.

142 Article 2 of Circular 420.

the DPO[143]. That assessment involves weighing the potential risks to the rights and freedoms of the data subject against the risks and freedoms of other data subjects and the risks of hindering the purpose and outcome of the processing operation[144]. Restrictions must be documented, including by recording the assessment of the rights restricted, for how long, for what reasons and on which grounds[145]. In addition, as long as a restriction applies, appropriate technical and organisational measures must be put in place[146]. Any restriction may only be applied for as long as the reasons for the restriction exist[147]. If a right is restricted, the controller must inform the individual of the principal reasons therefor and of the right to submit a complaint[148].

2.4.6.3. Specific rules in the context of the patent granting procedure

(55) Provisions of the constitutive treaty of the EPO (that is to say the EPC), of the PCT, and provisions applicable under them (all constituting primary legislation for the EPO) contain certain specific requirements in the context of the patent granting procedure that may impact the exercise of certain rights under the DPR[149]. The PGP Decision provides an overview of those primary legislation requirements, explains how data subject rights can be exercised in that context, and clearly sets out possible exceptions[150]. Circular 420 establishes that those provisions that may limit the application of data protection rights must clearly identify the scope of any exemption, and therefore balance the different interest at stake[151].

(56) First, pursuant to Article 127 of the EPC, the Office is obliged to maintain the European Patent Register, where certain legally defined personal data are published. According to primary legislation, patent applications must be published during the patent granting procedure, generally, as soon as possible after expiry of a period of eighteen months from the date of filing. The EPC provides that personal data included in such patent applications can either be accessed by means of file inspection or inspecting the Register[152]. Before publication, patent applications are

143 Article 25(3)(a) of the DPR. See also Article 6 of Circular 420.

144 Article 5(5) of Circular 420.

145 Article 4(4) of Circular 420. These records must be made available to the DPB upon request (Article 4(7) of Circular 420).

146 The measures must include for example secure storage, a secure electronic environment which prevents unlawful and accidental access to or transfer of electronic data to unauthorised persons and the monitoring of restrictions and periodic review of their application, see Article 5(2) of Circular 420.

147 Article 4(5) and 5(3) of Circular 420.

148 Article 25(3)(b) of the DPR. This information may be deferred, omitted, or denied if it would cancel the effect of the restriction, see Article 25(4) of the DPR. This further restriction can only be applied in duly justified cases and as long as and to the extent necessary and proportionate (Article 7(4) of Circular 420). The justification for such a restriction must be re-assessed on a regular basis. In addition to the specific requirement to inform individuals about a restriction of their rights, the EPO must provide general information on its intranet and/or website on the activities that may involve restrictions of rights (Article 7(1) of Circular 420).

149 Article 2 of Circular 420 (legal provisions of EPO).

150 Article 1 and Annex of the PGP Decision.

151 Article 2 of Circular 420.

152 Paragraph C.13 and C.14 Annex to the PGP Decision and Article 128 of the EPC. Parts of file excluded from file inspection Note that certain parts of files are excluded from file inspection according to Article 128(4) and Rule 144 of the Implementing Regulations to the EPC and the decision of the President of the EPO of 12.07.2007 concerning documents excluded from file inspection (Special edition No. 3, OJ EPO 2007, J.3) are the following: documents relating to the exclusion of or objections to members of the Boards of Appeal or of the Enlarged Board of Appeal; draft decisions and notices, and all other

not available for inspection without the explicit consent of the applicant. Similar rules are laid down in the PCT[153].

(57) Second, the possibility to obtain changes to information used in the context of a patent granting procedure is specifically regulated by the EPC[154]. In particular, the EPC only provides for the possibility to obtain the correction of errors in documents filed with the EPO[155], correction of errors in decisions[156], corrections of translations[157] and rectification of inventor designation[158]. The rectification of personal data included in documents used in the patent granting procedure can therefore also only be obtained in those cases. The same applies to the possibility to obtain a restriction of data processing[159].

(58) Thirdly, the EPC imposes specific retention and publication requirements for certain documents used in the patent granting procedure, which have an impact on the possibility to obtain deletion of information contained therein, including personal data[160]. In particular, published patent applications and patent information published in the European Patent Bulletin must be retained and kept publicly available[161]. As a result, erasure of personal data contained in those documents would go against fundamental legal obligations of the EPO (Article 129(a) EPC) and cannot be obtained. Other files must be kept by the EPO for a period specified in the EPC, which is in principle five years[162]. As long as that period applies, erasure of information contained in those files (including personal data) cannot be obtained.

---

documents, used for the preparation of decisions and notices, which are not communicated to the parties; the designation of the inventor, if he has waived his right to be mentioned and any other document excluded from inspection by the President of the European Patent Office on the ground that such inspection would not serve the purpose of informing the public about the European patent application or the European patent, such as: medical certificates; requests for exclusion from file inspection and related correspondence; information the publication of which be prejudicial to the legitimate personal or economic interests and would not comprise information of relevance for the application or patent or grant procedure.

153 See Article 3 of the Decision of the President of the EPO of 20.02.2019 concerning online file inspection of documents contained in the held by the EPO as receiving Office, International Searching Authority or Authority specified for supplementary search (OJ EPO 2019, A17). See in this respect Article 30 PCT as regards public access to files, as well as Rules 94 and 48 of the PCT. Those provisions are relied on by the EPO when it acts as competent office or authority under the PCT pursuant to Articles 151-153 of the EPC.

154 A correction or rectification pursuant to these provisions may result in the updating of entries in the European Patent Register and the European Patent Bulletin and of publications of the application or patent. However, it will not retroactively change the content of the file (which will continue to contain all submissions of parties and communications and decisions from the EPO). Nor will it result in the withdrawal or deletion of earlier publications (paragraph C.19 Annex to the PGP Decision). This also applies under Article 19 and 34 of the PCT, when the EPO acts as competent authority/office on the basis of Article 151-153 of the EPC.

155 Rule 139 of the Implementing Regulations to the EPC.

156 Rule 140 of the Implementing Regulations to the EPC. In decisions of the EPO, only linguistic errors, errors of transcription and obvious mistakes may be corrected.

157 Article 14(2), second sentence, of the EPC.

158 Rule 21 of the Implementing Regulations to the EPC. An incorrect designation of an inventor can be rectified upon request and only with the consent of the wrongly designated person and, where such a request is filed by a third party, the consent of the applicant for or proprietor of the patent.

159 Paragraph C.25 of the Annex to the PGP Decision.

160 Paragraphs C.22-C.23 of the Annex to the PGP Decision.

161 Article 129 of the EPC.

162 Rule 147 (4) and (5) of the Implementing Regulations to the EPC.

(59) Therefore, taking into account in particular their limited scope and conditions for their application, the restrictions to the exercise of rights that derive from the provisions referred to in recitals 55 to 58 can be considered to be limited to what is necessary and proportionate to ensure the correct functioning of the patent granting procedure, as required in the public interest for the fulfilment of the EPO's official tasks. To the extent that the EPC and the PCT do not specifically regulate the exercise of data protection rights, that is to say in all other scenarios than the ones described in recitals 55 to 58, the requirements of the DPR apply in full.

2.4.7. Onward transfers

(60) The level of protection afforded to personal data transferred from the Union to the EPO must not be undermined by the further transfer of such data to recipients in a third country or another international organisation.

(61) The DPR distinguishes between 'transmissions of personal data' (that is to say the sharing of data by the EPO with its contracting States) and 'transfers of personal data' (the sharing of data by the EPO with any other person or entity outside the EPO)[163].

2.4.7.1. Transmissions of data

(62) First, the DPR provides that a transmission of data to a national intellectual property office of an EPO contracting State may occur if the data is necessary for (a) the performance of the recipient's competence or exercise of official authority or (b) the transmission is necessary for the exercise of the EPO's official tasks/authority[164]. Those transmissions take place in the context of the patent granting procedure provided for under the EPC and the PCT[165].

(63) Second, the DPR allows a data transmission to a public authority of a contracting State of the EPO[166], where the data are necessary for the performance of that public authority's tasks and the transmission is compatible with the tasks and functioning of the EPO[167]. Such transmissions are not specifically required under the EPC or other legal instruments governing the patent granting procedure but may still be necessary for the performance of the EPO's tasks, for example the cooperation of the EPO with its contracting States through consultation processes; the secondment and deployment of experts; or the provision of information on the EPO's staff for the purpose of determining social benefits, tax requirements, etc. The DPO has prepared model clauses to be included in memoranda of understanding governing such transmissions, which, among other things, provide for data protection principles, limit further processing only for compatible purposes, provide for data

163 Article 3(1)(r) and (s) of the DPR.

164 Article 8(2) of the DPR.

165 See in particular Article 130, 131 and 135 of the EPC, as well as relevant Implementing Regulations under the EPC (for example R 148-150). See also Article 12, 18, 20 and 36 of the PCT, as well as Implementing Regulations Rules 22, 23, 23 bis, 44, 47 and 71.

166 For example, a national or local authority, as well as another body governed by public law, such as a hospital or university.

167 Article 8(1) of the DPR.

subject rights, as well as obligations with respect to data security and data breaches and independent oversight[168].

(64) In both scenarios described in recital 63, the recipient, pursuant to the DPR, must 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 or States[169]. The controller must, for each transmission, be able to demonstrate that such transmission is necessary and proportionate to the specific purpose for which it is shared[170]. According to guidance issued by the DPO, that means that the data to be shared must be minimised and limited to what is adequate, relevant and strictly necessary to achieve that purpose[171]. If there is any reason to assume that the legitimate interests of the individual concerned may be affected, the controller must establish that it is proportionate to transmit the personal data for that specific purpose, after having weighed the different interests at stake[172].

(65) With regard to those two scenarios, it is also important to note that all EPO contracting States are party to the European Convention for the Protection of Human Rights and Fundamental Freedoms, subject to the jurisdiction of the European Court of Human Rights, as well as party to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS no. 108).

(66) Finally, the DPR allows data transmissions to a processor located in the European Economic Area (EEA), provided compliance is ensured with the requirements laid down in the DPR for the engagement of processors[173].

2.4.7.2. Transfers of data

(67) The sharing of personal data with any entity outside of the EPO other than a public authority or national intellectual property office of the EPO's contracting States or a processor in the EEA is considered a 'transfer' of personal data, subject to specific requirements under the DPR[174]. Those requirements apply for instance to the sharing of data with processors outside the EEA, controllers located in or outside contracting States, public authorities in non-contracting States, and other international organisations. In general, the DPR requires that the level of protection guaranteed to individuals by the EPO is not undermined when data is transferred to third parties[175]. According to the guidance of the DPO, the 'protection afforded to the transferred personal data in the third country or international organisation must be essentially equivalent to that guaranteed in the DPR'[176].

168 Overview of the requirement of the EPO's model data protection clause for memoranda of understanding, available at https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-template-data-protection-clause-for-mous.pdf.

169 Article 8(3) of the DPR.

170 Article 8(4) of the DPR.

171 Explanatory Note 'EPO transmission and transfer of personal data' (Transmission and transfer note), available at https://link.epo.org/web/office/data-protection-and-privacy/en-explanatory-note-on-epo-transmission-and-transfer-of-personal-data.pdf, footnote 12.

172 Article 8(3) of the DPR.

173 Article 8(1), (2) and (5) of the DPR.

174 Article 9(1) of the DPR.

175 Article 9(1) of the DPR.

176 Paragraph 52 of the Transmission and transfer note. 'Third country' is defined by the DPR as a country that is not a contracting State to the EPC, see Article 3(1)(t) of the DPR.

(68) Pursuant to the DPR, a transfer of personal data outside the EPO may first of all take place if the country where the recipient is located, or the international organisation, ensures an adequate level of protection and if the transfer is solely done to allow the EPO to carry out tasks within its competence[177]. An adequacy decision is adopted by the President[178], who, in case of doubt, decides after consulting the DPO and the DPB[179]. The DPO has developed an 'adequacy referential' setting out the criteria for adequacy decisions[180]. In particular, the legal framework of the third country or international organisation must, in particular, provide for key data protection principles, data subject rights, rules on onward transfers, procedural and enforcement mechanisms, and redress for individuals. If an adequacy decision is adopted by the President, the transfer can take place without the implementation of additional safeguards[181]. Member States, as well as Norway, Iceland, Liechtenstein, all countries that benefit from an adequacy decision from the Commission[182] and the Union institutions and bodies are currently considered by EPO to provide an adequate level of protection[183].

(69) Pursuant to the DPR, in the absence of an adequacy decision, the controller or processor may transfer personal data to recipients outside the EPO only if the controller or processor has provided appropriate safeguards and on condition that enforceable data subjects' rights and effective legal remedies for data subjects are available[184]. Such appropriate safeguards can be included in administrative arrangements with public authorities or international organisations, in contractual clauses (after consultation of the DPB)[185] or certification mechanisms[186]. The DPO has developed an outline of provisions to be included in administrative arrangements[187]. A model data protection agreement for transfers to processors is also available[188]. According to the guidance of the DPO, the EPO must assess whether the data importer would be prevented from complying with its obligations under a transfer tool due to the legal framework it is subject to and, if necessary, put in place supplementary measures[189]. To carry out that assessment, the DPO recommends, in EPO's explanatory notes on transmission and transfer of personal

177 Article 9(2) of the DPR.

178 See Article 1(2)a of the DPR, in conjunction with Article 10(2)(a) of the EPC and Article 9(2) of the DPR.

179 Article 9(3) of the DPR.

180 Outline of the EPO adequacy referential, available at https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-adequacy-referential-methodology.pdf.

181 Footnote 49 of the Transmission and transfer note.

182 With the exception of the EU-US Data Privacy Framework.

183 See Decision of the President of the European Patent Office of 17 November 2022 concerning countries and entities considered to ensure adequate protection of personal data, available at https://www.epo.org/en/legal/official-journal/2022/12/a111.html.

184 Article 9(4) and (5) of the DPR.

185 In this respect, the guidance of the DPO refers to the standard contractual clauses adopted by the European Commission as providing a good overview of the safeguards to be included, see paragraph 51 of the Transmission and transfer note.

186 Article 9(5) of the DPR. See also paragraph 33 of the Transmission and transfer note.

187 Overview of the requirements of the EPO's Administrative Arrangement models, available at https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-epo's-administrative-arrangements-modules.pdf.

188 See Annex E to the general conditions of contract for the EPO, available at https://link.epo.org/web/general_conditions_of_contract_en.pdf.

189 Paragraphs 52-53 of the Transmission and transfer note.

data, to take into account relevant guidance of the EDPB and the European Data Protection Supervisor.[190]

(70) Pursuant to the DPR, for data transfers to countries or organisations benefiting from an adequacy decision, as well as for data transfers on the basis of appropriate safeguards, the EPO must demonstrate the necessity and proportionality of each transfer for the purpose of the processing[191]. In addition, the EPO must establish, after having weighed the various interests at stake, that the transfer is proportionate, if there is reason to believe that the data subjects' legitimate interests might be prejudiced[192]. In addition, it must be ensured (through contractual safeguards) that the recipient may only process or use the data for the purposes for which they were transferred and must delete the data as soon as the purpose has been achieved[193].

(71) Pursuant to the DPR, in the absence of an adequacy decision or of appropriate safeguards, the transfer of personal data outside the EPO is permissible 'only exceptionally' if a so-called 'derogation' applies under similar conditions as the ones in the corresponding provisions of Union data protection law[194]. That is the case when (a) the data subject has explicitly consented to the transfer[195]; (b and c) the transfer is occasional and necessary for the performance of a contract with or in the interest of the data subject (or for the implementation of pre-contractual measures at the data subject's request)[196]; (d) the transfer is necessary for the performance of a task in the exercise of the official activities of the EPO or in the legitimate exercise of official authority vested in the controller[197]; (e) the transfer is occasional and necessary for the establishment, exercise or defence of legal claims[198]; (f) the transfer is necessary in order to protect the vital interests of an individual, where the data subject is physically or legally incapable of giving explicit consent[199]; or (g) the transfer is made from a register intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for such consultation are fulfilled in the particular

190 Paragraph 54 of the Transmission and transfer note.

191 Article 9 (6) of the DPR. In case there is any reason to assume that the data subject's legitimate interest might be prejudice, the controller must establish that it is proportional to transfer for that specific purpose after having weighed in the various competing interests.

192 Article 9(6) of the DPR.

193 Article 9(6) of the DPR.

194 See Article 10 of the DPR, as well as paragraph 39 of the Transmission and transfer note.

195 Article 10(1)(a) of the DPR. The individual must in this case be informed of the possible risks due to the absence of an adequate level of protection and appropriate safeguards. This derogation cannot be relied on by the EPO in the exercise of its official activities (Article 10(2) of the DPR).

196 Article 10(1)(b)-(c) and (2) of the DPR. These derogations cannot be relied on by the EPO in the exercise of its official activities (Article 10(2) of the DPR).

197 Article 10(1)(d) of the DPR. Such official activities or authority must be established on the basis of the EPC or other applicable legal provisions of the European Patent Organisation (Article 10(4) of the DPR). This includes the processing necessary for Office's management and functioning or for the performance of obligations arising from the EPO's duty of co-operation with the contracting States. Transfers may for instance take place to fulfil obligations, for example, between the Office and national bodies, tax or customs administrations, financial supervisory authorities, and services competent for social security matters or for public health, for example in the case of contact tracing for contagious diseases (Article 10(6) of the DPR).

198 Article 10(1)(e) and (2) of the DPR.

199 Article 10(1)(f) of the DPR.

case[200]. By nature, and according to the guidance of the DPO, those derogations may not be relied on for systematic, regular transfers[201].

(72) Finally, as regards transfers of specific categories of data to countries or organisations that do not benefit from an adequacy decision, the President may further limit such transfers for important reasons relating to the legitimate exercise of the official authority vested in the Office[202]. So far, the President has not made use of such powers.

2.4.8. Accountability

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

(74) Article 4(1) DPR establishes a general principle of accountability, making clear that the controller is responsible for, and must be able to demonstrate, compliance with the DPR. In particular, the controller must implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance, taking into account the nature, scope, context and purposes of processing and the varying likelihood and severity of any risks for the rights of individuals[203]. In that respect, the DPR also implements the principles of privacy by design and by default by requiring the controller to implement measures designed to implement the data protection principles and ensure compliance with the DPR, and to ensure that, by default, only personal data that is necessary for each specific purpose of processing is processed[204].

(75) The controller and processors must maintain a record of processing activities, containing, among other things, information on the purpose of processing, the categories of data processed, the categories of recipients to whom data is disclosed, and any transfers of personal data[205]. Those records are in principle publicly accessible (unless they contain confidential information), and included in a publicly available Data Protection Register, and must be made available to the DPB on request[206]. Each operational unit must also appoint at least one Data Protection Liaison (for a renewable term of one to three years), who must undergo compulsory

---

200 Article 10(1)(g) of the DPR. Such a transfer may not involve the entirety of the personal data or entire categories of the data contained in the register, unless authorised by legal provisions of the European Patent Organisation, and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject (Article 10(2) and (5) of the DPR).

201 Paragraph 42 of the Transmission and transfer note.

202 Which, as mentioned before, includes the processing necessary for its management and functioning, or in reason of obligations deriving from its duty of co-operation with the contracting States. See Article 10(6) of the DPR.

203 Article 26(1) of the DPR.

204 Article 27(1) and (2) of the DPR.

205 Article 32(1) and (2) of the DPR. (1) Pursuant to Article 4(1) of the DPR, the controller must follow 'a structured and risk-based approach to designing and documenting processing operations'. The controller must also be able to demonstrate to data subjects at all times that the documented commitments and conditions are observed when processing operations are carried out.

206 Article 32(4), (5) and (6) of the DPR.

data protection training and assist the controller in complying with its obligations[207].

(76) Finally, the DPR provides different instruments that can assist the controller and processors in their compliance efforts. For example, pursuant to the DPR, adherence to approved certification mechanisms may serve as evidence of compliance with DPR obligations[208]. In addition, under certain conditions, the DPR requires carrying out a data protection impact assessment, or a prior consultation of the DPO and DPB. A data protection impact assessment is required where a type of processing is likely to result in a high risk to the rights and freedoms of an individual[209]. That is, for instance, required where there is a systematic and extensive evaluation of personal aspects on which automated decisions are based, or there is processing of special categories of data on a large scale[210]. If an impact assessment indicates that the processing would result in a high risk for the rights and freedoms of individuals and the risk cannot be mitigated by reasonable security measures, the controller must consult the DPB[211]. The DPB must provide written advice if it is of the opinion that the intended processing would be in violation of the DPR[212]. More generally, the controller is required to consult the DPO when preparing rules or operational documents on the implementation of restrictions to individual rights[213].

2.5. Oversight and enforcement

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

(78) The legal framework of the EPO entrusts two bodies with the oversight of compliance with the data protection rules by the EPO: the DPO and DPB. Both bodies are created by Article 32A of the Service Regulations, while their status and powers are further specified in the DPR[214].

2.5.1. Independence

(79) Pursuant to the Service Regulations, the DPO and DPB act completely independently of any internal or external interference in performing their tasks and

207 Article 45 of the DPR.

208 Article 26(3) of the DPR.

209 The controller must seek the advice of the DPO on the need to carry out an impact assessment, who may in turn consult the DPB in case of doubt. See Article 38(1)-(2) of the DPR.

210 Article 38(4) of the DPR.

211 Article 38(6) of the DPR.

212 Article 38(7) and (8) and Article 39 of the DPR.

213 Article 40(2) of the DPR.

214 Article 32A(1)-(2) of the Service Regulations, which provides that the role of the DPO is to monitor the application of the provisions on the protection of personal data, advise the various operational units of the EPO on fulfilling their obligations and to provide them with operational documentation necessary for the practical implementation of data protection requirements. The DPB is required to ensure 'independent, effective and impartial oversight of the provisions applicable to the protection of personal data'. A different independent oversight mechanism may exist to oversee compliance by the Boards of Appeal when processing personal data in its judicial capacity (see also Article 2(6) of the DPR).

exercising their powers[215]. That principle is complemented by different additional safeguards that guarantee their independence.

(80) The DPO (and their deputies) are appointed by the President on the basis of their professional qualifications and, in particular, their expert knowledge of data protection law and practices[216]. The DPO is appointed for a renewable term of three to five years. The DPB shall be consulted prior to any proposed removal or dismissal of the DPO from his or her role[217]. Such prior consultation before removal or dismissal of the DPO is designed to ensure additional scrutiny and review in case of proposed removal or dismissal. Such removal or dismissal can be put forward for one of the following reasons[218]: where the DPO no longer fulfils the conditions required for the performance of the duties[219]; for professional incompetence[220]; or as a result of disciplinary measures[221]. The DPO cannot be dismissed or penalised for performing its tasks and cannot receive any instructions[222]. The DPO must be involved in all issues relating to the protection of personal data and issues annual activity reports to the President and the Administrative Council[223]. The Office must provide the DPO with the resources necessary to carry out its tasks[224].

(81) The DPB is composed of three external experts in the field of data protection, namely a chair and two other members[225], as well as an alternate member, appointed by the EPO President for a renewable term of three years[226]. DPB members must have the qualifications required for appointment for judicial office or be data protection professionals with proven expertise and experience in the area of data protection law acquired at national or international level. They may not be

---

215 Article 32A(4) and (5) of the Service Regulations.

216 Article 41 of the DPR.

217 Article 42(8) of the DPR.

218 Article 50 of the Service Regulations.

219 See Article 53(1) of the Service Regulations, stating that '[t]he appointing authority may decide to terminate the service of an employee: (a) if the contracting State of which the employee is a national ceases to be party to the Convention; (b) if the employee refuses to be transferred to a country other than that in which he is serving; (c) if, in the case of an employee appointed by the Administrative Council in accordance with Article 11, paragraphs 1 and 2, of the Convention, the Administrative Council so decides in the interests of the Organisation; (d) who has been in continuous service for one year or less on a fixed-term appointment; (e) if as a result of his own actions, he ceases to fulfil the conditions laid down in Article 8, sub-paragraph (a) or (b) [that is to say being a national of one of the EPO contracting States, unless an exception is authorised by the appointing authority, and enjoying full rights as a citizen]; or (f) in the other cases expressly provided for in these Service Regulations'.
See also Article 13(4)(b) of the Service Regulations, stating that 'A report on the probationer may be made at any time during the probationary period, if the fulfilment of his duties, his efficiency and his conduct are proving inadequate. On the basis of the probationary report or reports, the appointing authority may:
- dismiss a new recruit on probation,
- decide that the probationer who has been transferred, promoted or reassigned shall return either to his previous post or, if this has been filled, to a post corresponding to the grade of his previous post for which he satisfies the requirements'.

220 Article 52 of the Service Regulations.

221 Article 94 of the Service Regulations.

222 Article 42(3) of the DPR. While the DPO may also fulfil other tasks, such tasks may not result in a conflict of interest (Article 42(6) of the DPR).

223 Article 42(1) and (3) of the DPR.

224 Article 42(2) of the DPR.

225 Article 48 (1) of the DPR.

226 Article 48(1) and (3) of the DPR.

employees of the EPO or have been employed by it within the past ten years[227]. Pursuant to Article 48(6) DPR, the members of the DPB are completely independent in carrying out their function. In particular, DPB members may not seek instructions from the Office or the Administrative Council and cannot be bound by such instructions. The Rules of Procedure of the DPB also provide that it must act impartially and with complete independence when performing its tasks[228]. Moreover, DPB members can only be terminated by EPO from their position for serious cause[229]. DPB members are bound by an obligation of confidentiality[230] and must refrain from acting in a case in which they have a conflict of interest, in particular a personal interest[231]. The EPO is required to support the DPB in performing its tasks by providing it with the necessary resources, as well as legal and administrative support (through a Secretariat and by providing the DPB with access to personal data and processing operations)[232].

2.5.2. Tasks and powers

(82) The tasks of the DPO include the following: informing the controller or processors of their obligations and advising them accordingly; raising awareness among and providing training for staff involved in processing operations; ensuring that data subjects are informed of their rights under the DPR; and monitoring in an independent manner the internal application and compliance with the DPR, as well as other legal provisions of the EPO having data protection implications[233]. Data subjects may contact the DPO on any issue relating to the processing of their data or the exercise of their rights, and the controller and processors may consult the DPO on any matter concerning the interpretation and application of the DPR[234].

(83) As part of its oversight role, the DPO has the power to carry out data protection audits and investigations[235]. Audits are initiated by the DPO in accordance with an annual audit plan that is prepared in consultation with the DPB[236]. An audit focuses on assessing data protection records, statements and relevant documentation, for instance, to verify the accuracy and completeness of relevant data protection documentation, the correct application of risk management methodologies, the accuracy and timeliness of responses to data subjects, or the proper conduct and the

227 Article 48(2) of the DPR.

228 Article 1(1) of the Rules of Procedure of the Data Protection Board, CA/26/21 Add. 1, adopted on 11 June 2021. Available at https://link.epo.org/web/data_protection_board-rules_of_procedure_en.pdf

229 In particular, the agreement provides that it 'may [only] be terminated, without prejudice to the right to terminate for serious cause, by the [DPB Member] upon six (6) months' written notice'. Since the service agreement is regulated by German law, the notion of serious cause must be interpreted in accordance with §626 of the German Civil Code. According to case law, this may for instance be fulfilled in case of repeated and persistent violation of applicable obligations (for example regarding conflict of interest) or imprisonment.

230 Article 48(5) of the DPR.

231 Article 48(7) of the DPR.

232 Article 48(10) of the DPR. The Secretariat performs its tasks independently from any undue interference and exclusively under the instructions of the Chair of the DPB. It provides legal, administrative, and logistical support to the Board. See Article 2 Rules of Procedure of the DPB.

233 Article 43(1) of the DPR.

234 Article 42(4) and (7) of the DPR.

235 Article 43(1)(d) DPR. See also the Data protection oversight note 'How the Data Protection Office Conducts DP Audits and DP Inspections', available at https://link.epo.org/web/office/data-protection-and-privacy/en-outline-of-the-data-protection-oversight-mechanism.pdf.

236 The DPB can formulate suggestions on areas on which audits should be performed, see Data protection oversight note, p. 4.

number of data protection impact assessments[237]. According to information received by the Commission from the DPO, three audits were conducted in 2023 and four in 2024. An investigation can be initiated by the DPO on its own initiative, on the basis of a request received from the DPB or a body within the EPO (for example the President or a delegated controller), or on the basis of information otherwise received (including for example from third parties and individuals)[238]. Inspections focus on processing operations or particular aspects thereof or occurrences related thereto, with a view to ensuring that the processing in question meets the requirements of the DPR and to ensure the protection of the rights and freedoms of data subjects[239].

(84) The DPO has access to all relevant information, including the personal data being processed as well as all offices, data-processing installations and data carriers[240]. All EPO employees and operational units are required to assist the DPO in performing its duties, including by providing access to premises and relevant information[241].

(85) When concluding an audit or investigation, the DPO adopts a report setting out its findings, conclusions and recommended remedial measures[242]. Such measures may for instance include preventative or mitigating measures to improve compliance, as well as measures to remedy non-compliance (for example to bring processing in compliance with the DPR, to handle requests from data subjects to exercise their rights, to suspend or terminate a processing, etc.)[243]. The DPO may also bring failures to comply with the DPR by employees to the attention of the competent appointing authority and recommend launching an administrative investigation to determine whether disciplinary or other action is needed[244]. Any employee failing to comply with the DPR, whether intentionally or through negligence, may be liable to disciplinary sanctions or other action pursuant to the Service Regulations[245].

(86) The outcome of audits and investigations must be communicated to the DPB[246]. The audit or investigation report must be shared with the DPB upon request. The DPB is allowed to comment on the DPO's report, including on the DPO's findings as to whether or not a violation of the DPR occurred, on proposed remedial measures, and it can request additional investigative measures[247]. If an audit or inspection by the DPO concludes that there has been a non-compliance (that is to say a violation of the DPR), the DPO's report must be submitted to the DPB for validation of the conclusions and the recommended remedial measures. In case of disagreement by the DPB with the conclusions or recommended remedial measures of the DPO, the DPB share its comments with the DPO, including to amend the

237 Data protection oversight note, p. 4.
238 Data protection oversight note, p. 7.
239 Data protection oversight note, p. 6.
240 Article 43(5) of the DPR.
241 Article 46 of the DPR.
242 Data protection oversight note.
243 Data protection oversight note, p. 2 (definition of 'recommendations').
244 Article 43(6) of the DPR.
245 Article 54 of the DPR. Disciplinary sanctions are imposed by the President, who exercises disciplinary authority and has disciplinary powers with respect to the EPO's staff, see Article 10 of the EPC and Article 93 et seq. of the Service Regulations.
246 Data protection oversight note, p.7.
247 Data protection oversight note, p. 3-4 and p. 8.

proposed conclusions and recommended remedial measures, which should implement them accordingly. Remedial measures that are validated by the DPB are binding towards the controller and delegated controllers and can be invoked by individuals before the redress mechanisms described in recital 94[248]. The DPO must verify the implementation of the remedial measures (in principle after six months from their communication) and report annually to the President on the status of implementation[249].

(87) In addition to its role to enforce compliance with the DPR, other tasks of the DPB include advising the President on the adoption of adequacy decisions, advising the controller on the need to carry out a data protection impact assessment and reviewing complaints from individuals (see recitals 91 to 93)[250].

2.6. Redress

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

(89) The legal framework of the EPO offers redress to individuals through a combination of different avenues.

(90) Firstly, data subjects who believe that the processing of their personal data by the EPO infringes their rights (that is to say violates the DPR) may submit a request for review by the delegated controller in accordance with Article 49 of the DPR. The delegated controller will review the complaint and take a decision[251]. Before taking a decision, the delegated controller must consult the DPO, who provide a written opinion no later than fifteen calendar days after receipt of the request for review[252]. The delegated controller must respond to the individual within one month from the date of receipt of the request[253]. The decision must be communicated to the individual, together with information on the possibility to obtain further redress[254]. If the delegated controller fails to take any action within three months, this is considered an implicit rejection of the request.

(91) Secondly, individuals may challenge a decision or an implicit rejection of a request for review by a delegated controller by filing a complaint with the DPB[255].

---

248 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, https://link.epo.org/web/office/data-protection-and-privacy/en-decision-of-the-president-on-enforceability-of-dpo-conclusions-and-recommendations.pdf.

249 Data protection oversight note, p. 5 and 9.

250 Article 47 of the DPR.

251 Article 49(1) of the DPR. A request must be submitted no later than three months from the day on which the data subject was informed or otherwise became aware of the processing of personal data allegedly infringing his or her rights.

252 Article 49(2) of the DPR. If the DPO does not provide an opinion by the end of this period, the opinion is no longer required.

253 Article 49(3) of the DPR. This time limit may be extended by two further months where necessary, taking into account the complexity and number of requests. In case of extension, the delegated controller must notify the data subject of this and the reasons for the delay within one month of receipt of the request for review.

254 Article 49(3) of the DPR.

255 Article 50(1) of the DPR. A complaint before the DPB must be submitted within three months of the receipt of the decision or, in case of an implicit rejection, of the date of the expiry of the time limit for replying to the request.

(92) When examining a complaint, the DPB must invite the data subject, the controller and, where applicable, the processor to set out in writing their position on the claims and facts at issue and to provide evidence or comments and arguments on available evidence[256]. In that context, the DPB may request any information it needs from the parties to handle the complaint and can, in addition, obtain further information through the DPO[257]. In deciding on the necessary follow-up to a complaint, the DPB must take into account, among other things, the nature and gravity of the alleged infringement, the number of data subjects affected, the categories of data affected and the duration of the infringement[258]. The DPB may invite the parties to seek an amicable settlement and encourages and actively facilitates such settlement[259]. The complainant may also ask the DPB to apply an urgency procedure, for reasons of gravity of the alleged infringement or due to the severity of the risk imposed on the rights of individuals[260].

(93) After examining a complaint, the DPB issues a reasoned opinion to the controller, which shall include a statement of facts, the main arguments of the parties, the DPB's considerations and its recommendations[261]. In case of an urgency procedure, the DPB must issue a reasoned opinion within two months of the lodging of the complaint[262]. In its reasoned opinion, the DPB can issue any recommendations it considers necessary, including injunctive relief (for example terminating unlawful data processing, deleting unlawfully processed data), compensation for material or non-material damage[263]. The reasoned opinion must be communicated to the controller (that is to say the President or the Chair of the Administrative Council, depending on whether the complaint concerned the Office or the Council), which must provide written reasons to the DPO and DPB in case the opinion is not followed[264]. The reasoned opinion of the DPB and the final decision of the controller must be communicated by the controller to the data subject (and the delegated controller concerned)[265].

(94) A data subject that is not satisfied with the decision by the controller can appeal it further. Employees of EPO can challenge the decision before the Administrative Tribunal of the International Labour Organisation[266]. Any other data subject that disagrees with the decision of the controller can, within three months of the receipt of the decision, submit a request to the President for ad-hoc arbitration[267]. The DPR provides for a specific procedure to be followed in case of ad hoc arbitration[268]. In particular, within three months of receipt of the request by the data subject, one

256 Article 50(2) of the DPR.

257 In particular, the DPO is under an obligation to respond to requests from and cooperate with the DPB (Article 43(j) DPR). The DPO is also required to facilitate cooperation between the DPB and the Office and in that context has access to any relevant information (Article 46(a) and (b) of the DPR).

258 Article 4(5) of the Rules of Procedure of the DPB.

259 Article 8 of the Rules of Procedure of the DPB.

260 Article 11 (1) of the Rules of Procedure of the DPB.

261 Article 10(2) of the Rules of Procedure of the DPB.

262 Article 11 (2) of the Rules of Procedure of the DPB.

263 Article 50(3) of the DPR.

264 Article 50(4) of the DPR.

265 Article 50(6) of the DPR.

266 Article 50(7) of the DPR. See Article 13 of the EPC and Article 113 of the Service Regulations.

267 Articles 50(8) and 52 (2) of the DPR. Under the AC DPR and the SC DPR, arbitration can be requested from the Chair of the AC.

268 Article 52(1) of the DPR.

arbitrator must be appointed by the Secretary-General of the Permanent Court of Arbitration based on criteria laid down in the DPR[269]. The arbitrator must be legally qualified, admitted to practice law in one of the EPO's contracting States, be able to demonstrate relevant expertise in data protection matters and be familiar with the law governing international organisations[270]. In addition to fulfilling those criteria, only individuals who have not worked for or at the service of either the EPO or the data subject may be appointed. The DPR provides that the arbitrator must act independently and impartially[271], treat each party equally and give them the opportunity of presenting their case at every stage of the proceedings[272]. The arbitration proceedings are not public[273] and are governed by the EPC, the DPR, including any implementing legislation, the law of international organisations and the principles of public international law[274]. While each party has to bear its own costs and expenses for legal representation (unless the arbitrator decides otherwise), the arbitrator's fees and expenses, the cost of possible expert advice and witnesses are paid by the EPO[275]. A settlement must be concluded in the form of a written arbitration award with an agreed wording, which is final and binding[276].

(95) Any individual that has suffered damage as a result of a violation of the DPR may request compensation from the EPO using the procedures described in recitals 90 to 94[277]. The EPO will not be held liable if it proves that it was not responsible for the event giving rise to the damage.

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

(96) The legal framework under which the EPO assesses and responds to requests from public authorities – in its contracting States and in third countries – concerning personal data processed by the EPO follows from the EPO Protocol on Privileges and Immunities (PPI)[278], the DPR requirements on transmissions and transfers of personal data, and public international law.

(97) Firstly, the processing of personal data by the EPO for the purpose of its official activities is covered by the Organisation's immunities. EPO's immunities are complemented by a duty of cooperation set out in Article 20 of the PPI. Consequently, any request from a public authority of a contracting State to obtain data processed by the EPO assessed by the President in accordance with (Article

269 Article 52(4) of the DPR.
270 Article 52(4) of the DPR.
271 Article 52(4) of the DPR.
272 Article 52(8) of the DPR.
273 Article 52 (9) of the DPR.
274 Article 52(6) of the DPR. The place of arbitration is The Hague (Article 52(5) of the DPR) and the language used during the proceedings must be chosen by the arbitrator, which must, however, be one of the official languages of the EPO (English, French or German) (Article 52(7) of the DPR).
275 Article 52(13) of the DPR.
276 Article 52(10) of the DPR. See also Article 3 and 34(2) of the Rules of Permanent Court of Arbitration.
277 Article 53 of the DPR. Under certain conditions (in particular applicable requirements under German law), individuals can also obtain compensation for damages caused by EPO staff in the performance of their duties, pursuant to Article 9(2) of the EPC.
278 Protocol on Privileges and Immunities of the EPO. Available at https://www.epo.org/en/legal/epc/2020/proprim.html

20(1)) of the PPI, which provides that the Organisation 'shall co-operate at all times with the competent authorities of the Contracting States in order to facilitate the proper 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.' As an exception, the Organisation may waive its immunity from jurisdiction and execution[279]. When deciding on a request for cooperation, the President exercises discretion. The conclusion may be that the Office can respond to a request under the PPI and may only disclose personal data in compliance with the requirements for transmissions of data provided for in the DPR (see recitals 62 to 66). Pursuant to the DPR, the recipient must 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(s)[280]. The controller must, for each transmission, be able to demonstrate that such transmission is necessary and proportionate to the specific purpose for which it is carried out[281]. According to guidance issued by the DPO, that means that the data to be shared must be minimised and limited to what is adequate, relevant and strictly necessary to achieve that purpose[282]. If there is any reason to assume that the rights and freedoms of the individual concerned may be affected, the controller must establish that it is proportionate to transmit the personal data for that specific purpose, after having weighed the different interests at stake[283].

(98) Secondly, there is no legal instrument applicable to the EPO that specifically regulates the handling of requests from public authorities of third countries (that is to say that are not a contracting party to the EPO) to obtain data processed by the EPO. As a result, any disclosure in response to such a request can only take place if the requirements for international data transfers under the DPR (as described in recitals 67 to 72) are met. That would only be the case if an adequacy decision has been adopted for the relevant country that would cover the transfer, if appropriate safeguards are in place, or if a derogation applies.

(99) Compliance by the President with the PPI is subject to the supervision of the Administrative Council, whereas compliance with the requirements on transmissions and transfers of personal data in the DPR is subject to the oversight of the DPO and the DPB, as described in recitals 83 to 87. Individuals can make use of the redress avenues described in recitals 89 to 95 concerning transmissions or transfers of their personal data in violation of the DPR.

4. CONCLUSIONS

(100) The Commission considers that the EPO ensures a level of protection for personal data transferred from the Union, that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.

(101) On the basis of the findings of this Decision, it should be decided that the EPO ensures an adequate level of protection within the meaning of Article 45 of

279 Article 3(1)(a) of the PPI.
280 Article 8(3) of the DPR.
281 Article 8(4) of the DPR.
282 Transmission and transfer note, footnote 12.
283 Article 8(3) of the DPR.

Regulation (EU) 2016/679, interpreted in light of the Charter of Fundamental Rights of the European Union, for personal data transferred from the Union to the EPO.

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

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

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

(104) It should be recalled that, pursuant to Article 58(5) of Regulation (EU) 2016/679 and as explained by the Court of Justice in Case C-362/14[284], where a national data protection authority questions, including upon a complaint, the compatibility of a Commission adequacy decision with the fundamental rights of the individual to privacy and data protection, national law must provide it with a legal remedy to put those objections before a national court which may be required to make a reference for a preliminary ruling to the Court of Justice.

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

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

(106) Therefore, the Commission should on an on-going basis monitor the situation as regards EPO's legal framework and actual practice for the processing of personal data, as assessed in this Decision. To facilitate this process, the EPO is invited to inform the Commission of material developments relevant to this Decision, as regards the processing of personal data and the limitations and safeguards applicable to access to personal data by public authorities.

(107) Moreover, in order to allow the Commission to effectively carry out its monitoring function, the Member States should inform the Commission about any relevant action undertaken by the national data protection authorities, in particular regarding queries or complaints by Union data subjects concerning the transfer of personal data from the Union to the EPO.

[284] Case C-362/14, Schrems ('Schrems I'), ECLI:EU:C:2015:650, paragraph 65.

(108) In application of Article 45(3) of Regulation (EU) 2016/679, and in the light of the fact that the level of protection afforded by the EPO's legal framework may be liable to change, the Commission, following the adoption of this Decision, should periodically review whether the findings relating to the adequacy of the level of protection ensured by the EPO are still factually and legally justified. Such evaluations should take place at least every four years and should cover all aspects of the functioning of this Decision, including the functioning of the relevant oversight and enforcement mechanisms.

(109) To perform the review, the Commission should meet with the EPO, including its DPO and the DPB. Participation in that meeting should be open to representatives of the members of the European Data Protection Board. In the framework of the review, the Commission should request the EPO to provide comprehensive information on all aspects relevant for the adequacy finding. The Commission should also seek explanations on any information relevant for this Decision that it has received, including from the EDPB, individual data protection authorities, civil society groups, public or media reports, or any other available source of information.

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

(111) Where available information, in particular information resulting from the Commission's monitoring of developments that could affect the functioning of this Decision pursuant to Article 45(4) of Regulation (EU) 2016/679 or provided by the EPO or Member States' authorities reveals that the level of protection afforded by the EPO may no longer be adequate, the Commission should inform the EPO thereof and request that appropriate measures be taken within a specified, reasonable timeframe.

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

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

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

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

7. FINAL CONSIDERATIONS

(116) [PLACEHOLDER: The European Data Protection Board published its opinion[285], which has been taken into consideration in the preparation of this Decision.]

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

HAS ADOPTED THIS DECISION:

Article 1

For the purpose of Article 45 of Regulation (EU) 2016/679, the European Patent Organisation ensures an adequate level of protection for personal data transferred from the Union to the European Patent Organisation.

Article 2

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

Article 3

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

2. The Member States and the Commission shall inform each other of cases where the European Patent Organisation fails to ensure compliance with the legal framework upon which this Decision is based.

4. At least every four years, the Commission shall evaluate the finding referred to in Article 1 on the basis of all available information, including the information received as part of a review carried out together with the European Patent Organisation.

5. Where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the European Patent Organisation thereof. If necessary, the Commission may decide to suspend, amend or repeal this Decision, or limit its scope, in accordance with Article 45(5) of Regulation (EU) 2016/679.

   The Commission may also suspend, repeal or amend this Decision if the lack of cooperation of the European Patent Organisation prevents the Commission from determining whether the assessment referred to in Article 1(1) of this Decision is affected.

Article 4

[285] PLACEHOLDER.

This Decision is addressed to the Member States.

Done at Brussels,

For the Commission

Michael McGRATH

Member of the Commission