Europäische Patent-organisation
Verwaltungsrat

European Patent Organisation
Administrative Council

Organisation européenne des brevets
Conseil d'administration

CA/26/21
Orig.: en
Munich, 11.06.2021

SUBJECT: Modernisation of the data protection framework of the European Patent Office under the Strategic Plan 2023

SUBMITTED BY: President of the European Patent Office

ADDRESSEES: Administrative Council (for decision)

SUMMARY

This document proposes a modernised data protection framework for the EPO. The Administrative Council is requested to adopt amendments to the Service Regulations as well as new Data Protection Rules based on them. The Council is further requested to note the Rules of Procedure of the new Data Protection Board set up to advise data controllers, including in complaints procedures (CA/26/21 Add. 1).

The proposal provides for a self-contained set of rights for staff and users, as well as procedures for effectively protecting these rights. This will endow the EPO with a solid and future-proof system of data protection that is on a par with the data protection standards of other international organisations, and in particular the EU data protection regime applicable to EU institutions and in most EPC contracting states. At the same time, the new framework reflects the EPO's specific tasks and institutional set-up. Applicable to data processing by the EPO, the new framework ensures the independence of the Boards of Appeal and preserves the Council's prerogatives regarding its own data processing.

Given the numerous changes introduced by the new framework, a staged transitional regime is envisaged: while the new framework is to enter into force on and apply to data processing operations as from 1 January 2022, there is a general six-month window for aligning ongoing data processing operations with the new requirements. This transition will also allow for consulting users on potential procedural changes.

TABLE OF CONTENTS

PART I

I. STRATEGIC/OPERATIONAL

1. Strategic

II. RECOMMENDATION

2. The Administrative Council is requested to:

- approve the amendments to the Service Regulations in Part II
- approve the Implementing Rules for Articles 1b and 32a of the Service Regulations (Data Protection Rules) in Part II
- note the Rules of Procedure for the Data Protection Board in Addendum 1.

III. MAJORITY NEEDED

3. Three-quarters majority.

IV. CONTEXT

4. As an international organisation, the European Patent Organisation has an obligation to consider the wider impact of its actions when contemplating how to meet future challenges. As envisaged in its Strategic Plan 2023 (SP2023),[1] the Office pursues an approach that creates long-term value, not only in terms of its financial sustainability, but also in terms of environmental and social sustainability.

5. The outbreak of the COVID-19 pandemic has substantially changed the circumstances under which EPO conducts its activities and greatly accelerated the pace of digital transformation. Communication networks, data analytics, cloud solutions and remote devices are employed today on a large scale, as part of the Office's efforts to best manage the crisis, increasing the need for effective guarantees concerning data protection and privacy.

6. More than ever, the EPO needs to rely on digital approaches to its daily activities. Technologies designed to increase convenience and prosperity – from behavioural analytics to facial recognition – have a potentially negative impact when used for surveillance and targeting. The increased dependency on data and technology amplifies the pre-existing conditions of EPO digital systems, including the dependency on software providers, outsourcing of certain services, and exposure to data breaches.

7. The right to privacy and to the protection of personal data are fundamental human rights. As a socially responsible organisation, the Office's mission and values are to treat people – employees, users, partners and other stakeholders – with respect and in line with the duty of care.

[1] CA/65/19.

8. In this context, as part of SP2023, the EPO envisaged a comprehensive review of its data protection framework, starting with the rules regulating data protection and the adoption of new Data Protection Rules (DPR) to align the Office with the principles and key requirements of global best practice in the area of data protection[2].

9. The implementation of a solid legal framework is the first step towards ensuring adequate protection and mitigation of risks. A risk-based approach to the implementation of further technical measures and specific instructions and awareness raising among managers and staff to support them in their role and responsibilities as data controllers and processors will be the pillars of the EPO's new strategy towards data protection.

10. In its commitment to excellence and sustainability, the EPO aims to address data governance as a mean of ensuring high-quality and full-scope application of the protection of personal data.

11. Demonstrating compliance with the highest standards of protection and best practices is key for maintaining the trust of users, staff, EPO partners, stakeholders, and the public. The users who interact with the EPO entrust it with highly sensitive information. The EPO also processes the personal data of over 7 000 staff members and their families, among them many children, as well as the data of external contractors, training course participants and the Member States' delegates. Ensuring that the EPO has strong safeguards in place to protect their personal data is key for its functioning and its reputation.

12. The modernisation of the EPO's data protection framework also needs to support the EPO in carrying out its various tasks in the European and international patent system. Moreover, due consideration needs to be given to the EPO's institutional set-up, in particular the independence of the Boards of Appeal and the supervision of the Office by the Administrative Council.

V. ARGUMENTS

13. The current EPO Data Protection Guidelines (DPG) were last revised in 2014. Therefore, they do not take into account a number of significant data protection and privacy law developments in Europe and worldwide, all aiming to empower data subjects, enhance their rights, and assure them that their personal data are not being misused.

[2] CA/65/19, p. 88.

14. In an effort to harmonise the EPO's data protection framework with the practices and standards of international organisations and institutions, the new EPO DPR are aligned, wherever possible, with the EU General Data Protection Regulation (GDPR)[3], which has set arguably the most demanding data protection standard worldwide. The GDPR applies to the data of all individuals (also non-EU nationals) who are located within the EU at the time their data is processed, regardless of where the organisation processing the data is located, so that many of the EPO's users, contractors and partners are subject to it. Further consideration was given to Convention 108 of the Council of Europe, which has been signed by all contracting states to the European Patent Convention, as well as to the rules of other international organisations that have aligned their regimes with the highest standards in data protection[4].

15. The new DPR are not limited to updating or amending the existing guidelines. Rather, the objective of the Office is to create a modern, integrated data protection framework, for which the new DPR lay the foundations. The new, comprehensive regulations address specifically the following needs:

- Enshrine the data protection principles, in particular the principles of lawfulness, fairness, transparency and accountability, at the level of the Service Regulations and their Implementing Rules, thereby elevating the Data Protection Rules to the level of secondary legislation and enhancing the visibility of the Office's commitment to the protection of personal data for staff and the outside world.

- Define and clarify the roles of the different actors in the complex data processing mechanisms to raise awareness amongst stakeholders of their roles and responsibilities and of the risks associated with the processing of data and to assist managers and staff in ensuring the protection of the managed personal data.

- Strengthen and clarify the individual rights defined in the DPR, such as the right to information, right to access, right to object, right to data portability, right to erasure ("right to be forgotten"), to provide data subjects with more control over their personal data.

- Have effective mechanisms in place to prevent and efficiently address personal data breaches if they occur.

- Offer effective and timely redress mechanisms for data subjects, including external parties, affected by non-compliance with the provisions on the protection of personal data.

- Create within the EPO legal framework a body with an oversight function composed of external members (Data Protection Board) to monitor the processing of personal data by the Office and advise the President.

[3] EU Regulation 2016/679.
[4] Such as the Organisation for Economic Co-operation and Development (OECD) and the European Space Agency (ESA), and Regulation 2018/1725 of the European Union institutions (EUDPR).

16. The main elements of the revised Data Protection legal framework are outlined below.

A. FIELD OF APPLICATION OF DATA PROTECTION FRAMEWORK

17. The new data protection framework will apply to the processing of personal data by the Office (cf. Article 2(1) DPR). This leaves the Administrative Council's prerogatives regarding its own processing of personal data unaffected.

18. In line with the standards of the EU data protection rules,[5] data processing by the Boards of Appeal in their judicial capacity is subject to the new data protection framework, but it is excluded from the oversight mechanisms that the new framework puts in place for data processing by the Office (cf. Article 32a(7) ServRegs and Article 2(6) DPR). As such mechanisms may conflict with the judicial independence of the Boards of Appeal, independent oversight mechanisms will be established for the Boards of Appeal.

19. As regards the personal scope of application, the new framework will apply to the data of persons covered by Article 1 ServRegs and of natural persons not covered by Article 1 ServRegs (cf. Article 2(2) DPR).

B. PRINCIPLES OF DATA PROTECTION

20. The basic principles of data protection are enshrined in the Service Regulations or in their Implementing Rules:

- lawfulness, fairness, transparency and accountability: personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject, and the controller shall be responsible for, and be able to demonstrate compliance with the rules;

- purpose limitation: data shall only be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with these purposes;

- data minimisation: data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and processed;

- accuracy: data shall be accurate and, where necessary, kept up to date;

- storage limitation: data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data were collected or for which they are further processed;

- integrity and confidentiality: data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

[5] Cf. Article 55(3) GDPR; Article 57(1)(a) EUDPR.

C. CLARIFICATION OF THE CONCEPT OF CONSENT

21. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. The request for consent shall be presented in a manner which is clear and intelligible. Consent shall be freely given, specific, informed and unambiguous and the data subject shall have the right to withdraw consent at any time. Special protection is awarded to children.

D. CLARIFICATION OF OBLIGATIONS IN THE CASE OF TRANSFERS OUTSIDE THE EPO

22. In order to fulfil its tasks, the EPO is required to transmit and transfer data to outside entities. This includes transmissions and transfers to the EPO's external governance bodies, national and international authorities and, in particular, other patent offices as part of regular data exchanges within the European and international patent system. The new data protection framework facilitates these data flows while protecting data subjects' rights. Data may be transmitted to public authorities and patent offices of EPC contracting states in order for the EPO and the recipient to fulfil their respective tasks. When transferring data to other recipients, the EPO will additionally verify that such recipients offer adequate levels of protection and/or safeguards.

E. CLARIFICATION AND STRENGTHENING OF THE RIGHTS OF THE DATA SUBJECT

23. The rights of the data subject are clarified and strengthened, in particular:

- Right to information
- Right to access
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to object
- Specific provision addresses automated individual decision-making, including profiling

F. CLARIFICATION AND STREAMLINING OF THE ROLES OF DATA CONTROLLER AND DATA PROCESSOR

24. The roles of the data controller and data processor are streamlined and clarified. The accountability obligations of the controller translate into the duty to inform the data subject and to ensure that the data subject's above-mentioned rights are granted and protected. Furthermore, it is provided that the controller and the processor(s) put in place specific technical and organisational measures to ensure a level of security appropriate to the risk.

25. As a rule, the President of the Office acts as the controller for the data processing operations carried out by the Office, as follows from Article 10(2) EPC. However, where personal data are processed by the Boards of Appeal in their judicial capacity or in the exercise of the functions and powers delegated by the Act of Delegation,[6] the President of the Boards of Appeal acts as the controller. For data processing by the Boards of Appeal Unit in other contexts, the President of the Boards of Appeal acts as delegated controller. Except in the latter, specific case, the delegation and sub-delegation of controllership follows the EPO's established principles of delegation of powers (cf. Article 10(2)(i) EPC).

G. CREATION OF AN INDEPENDENT DATA PROTECTION BOARD (DPB)

26. The DPB's responsibilities include:

- monitoring, together with the Data Protection Officer, the due application of the provisions of the DPR and the administrative instructions to all data processing operations;
- issuing an opinion on the need for a data protection impact assessment following a request from the controller;
- establishing a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and a list of the kind of processing operations for which no data protection impact assessment is required;
- providing consultation and written advice to the controller on various issues.

H. STRENGTHENING THE ROLE AND INDEPENDENCE OF THE DATA PROTECTION OFFICER (DPO)

27. The Data Protection Board and the Data Protection Officer are granted independence from internal or external interference in performing their tasks and exercising their powers. The tasks and responsibilities of the DPO are exactly defined and thoroughly explained.

[6] OJ EPO 2018, A63.

I. CREATION OF DATA PROTECTION LIAISONS (DPLS)

28. As experts in the functioning of their operational units, the DPLs will assist the controller in complying with its legal obligations and ensure alignment with the DPO. The DPLs will serve as the Office's units' first point of contact for questions related to privacy and data protection, help the business owners to prevent personal data risks and incidents and offer the management a major advantage in the development and implementation of internal administrative procedures and measures related to personal data treatment.

J. CONFIDENTIALITY AND SECURITY PROCESSING

29. Provision is made for the controller and the processor(s) to put in place specific technical and organisational measures to ensure a level of security appropriate to the risk, including:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- the process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

K. SPECIAL CATEGORIES OF DATA

30. The definition of "special categories" of data includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership and data concerning health, as well as genetic or biometric data used to identify a natural person, and data concerning a person's sex life and sexual orientation. As a rule, processing of special categories of data is prohibited, except under certain clearly defined conditions.

L. DATA PROTECTION IMPACT ASSESSMENT

31. Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals by virtue of its context, nature, scope or purpose, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged appropriate measures to protect the personal data. This data protection impact assessment describes the processing operation and its purposes, the risks to the rights and freedoms of individuals and specific measures envisaged to address the risks.

M. DATA BREACH HANDLING

32. Under the new DPR, the controllers will have to efficiently tackle data breaches, such as personal data being made available to unauthorised recipients; this will include properly evaluating and mitigating them, notifying the DPO of them and, in some circumstances, also communicating them to the persons affected (so they can take steps to protect themselves). This requires clear differentiation between the concepts of "incidents" and "breaches" and a comprehensive procedure for the EPO to be able to comply with the strict deadlines applying where a data protection breach must be notified to the DPO and communicated to the data subjects affected. The main focus in this area is to be placed on proactive controls and preventive measures rather than on reactive response and mitigating actions.

N. LEGAL REDRESS

33. Specific means of legal redress are envisaged in cases of disagreement with an individual decision relating to a data subject, with a view to ensuring the protection of the rights, freedoms and interests of the data subjects, and minimising the financial and reputational risks for the EPO.

34. Except for data processed by the Boards of Appeal in their judicial capacity, to which independent oversight mechanisms apply, the data subject may request the delegated controller to review the matter and take a decision (Article 49 DPR). That decision can be challenged by filing a complaint with the DPB (Article 50(1) DPR). The controller takes a final decision taking into account the DPB's reasoned opinion (Article 50(3) DPR). It is ensured that the controllers keep each other informed of relevant decisions (cf. Article 50(5) DPR). As regards persons covered by Article 1 ServRegs, the aforementioned individual decisions taken by delegated controllers and controllers are excluded from the review and internal appeals procedures (Articles 109(3) and 110(2)(f) ServRegs), while the controller's final decision may be challenged before ILOAT (cf. Article 13 EPC). Persons not covered by Article 1 ServRegs have access to ad-hoc arbitration in order to challenge the controller's final decision (Article 52 DPR).

35. With regard to the relevant DPR articles, the following is to be noted:

a) With reference to Article 2 (Field of application) and 3 (Definitions):

- The concept of operational data as outlined in the previous provisions (Guidelines for the protection of personal data) is now obsolete and the DPR are fully applicable to the processing of such data. Therefore, the DPR do not contain any definition of "operational data".

- Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. All these may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

- The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The explicit introduction of "pseudonymisation" in the DPR is not intended to preclude any other measures of data protection.

- To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

b) With reference to Article 4 (Principles relating to processing of personal data): in order for processing to be lawful, personal data should be processed on the basis of the necessity for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation 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, the necessity for compliance with a legal obligation to which the controller is subject or some other legitimate basis under the DPR, including the consent of the data subject concerned, the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds relating to the performance of a task carried out in the exercise of the official activities of the European Patent Organisation 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, and the vital interests of the data subject, in particular in situations of natural and man-made disasters.

c) With reference to Article 6 (Processing for another compatible purpose): in order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the document concerned or reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

d) With reference to Article 7 (Conditions for consent): where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. A declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller.

e) With reference to Article 9 (Transfer of personal data): where the President did not render a decision whether the protection afforded by the country or international organisation in question can be considered adequate, the controller, delegated controller or processor should take measures to compensate for the potential lack of data protection by that third country or international organisation by way of appropriate safeguards for the data subject. Such appropriate safeguards can consist of EPO data processing agreements and data protection administrative arrangements and can also include the standard contractual clauses, binding corporate rules, codes of conduct and certification mechanisms used for international transfers under EU legislation. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. The possibility for the controller, delegated controller or processor to use EPO standard data processing agreements and administrative arrangements is not intended to prevent them from including the standard data protection clauses in a wider contract, such as a contract between the processor and another processor, or from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the EPO standard data processing agreement and administrative arrangement or prejudice the fundamental rights or freedoms of the data subjects. The controller, delegated controller and processor are encouraged to provide additional safeguards via contractual commitments and technical and organisational measures that supplement standard data protection clauses.

f) With reference to Article 11 (Processing of special categories of personal data):

- In addition to the specific requirements for processing of sensitive data, the general principles and other rules of the DPR shall apply, in particular as regards the conditions for lawful processing. Exemptions from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

- Special categories of personal data which merit greater protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems. Therefore, the DPR provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. The legal provision under Article 11(2)b. provides for specific and suitable measures so as to protect fundamental rights and the personal data of natural persons.

- The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, "public health" should be understood as all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, healthcare needs, resources allocated to healthcare, the provision of, and universal access to, healthcare as well as healthcare expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes.

g) With reference to Article 13 (Processing which does not require identification):

- If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of the DPR. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through an authentication mechanism such as the same credentials, used by the data subject to log in to the online service offered by the data controller.

- Modalities are provided for facilitating the exercise of the data subject's rights under the DPR, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object.

- The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

h) With reference to Article 16 (Information to be provided where personal data are collected from the data subject) and Article 17 (Information to be provided where personal data have not been obtained from the data subject):

- The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

i) With reference to Article 18 (Rights of access of the data subject):

- A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

j) With reference to Article 19 (Right to rectification) and Article 20 (Right to erasure ("right to be forgotten")):

- A data subject should have the right to have personal data concerning him or her rectified and a "right to be forgotten" where the retention of such data infringes the DPR or a legal provision to which the controller is subject. A data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with the DPR. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation or the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

- To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the other controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the other controllers which are processing the personal data of the data subject's request. Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

k) With reference to Article 22 (Right to data portability): to further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. The data controller is encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It is therefore not to be applied where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or in the exercise of the official activities of the European Patent Organisation or the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controller to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with DPR. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in the DPR and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

l) With reference to Article 24 (Automated individual decision-making, including profiling):

- The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as e-recruiting practices without any human intervention. Such processing includes "profiling" that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

- However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by the applicable EPO rules and regulations. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject. and prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

m) With reference to Article 34 (Notification and communication of a personal data breach):

- A violation of the DPR that does not constitute a personal data breach under Article 34 (e.g. no adequate legal basis, no notice to data subjects, etc.) does not fall under the obligations relating to personal data breaches, but it is still a violation of the DPR. A breach of information security which does not compromise personal data does not fall within the scope of these obligations. Whether the breach was intentional or not is irrelevant.

- The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play in enabling the controller to comply with its obligations; this includes breach notification. If a processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the risks arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered "aware" once the processor has informed it of the breach.

- A personal data breach could, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify that personal data breach to the Data Protection Officer without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, it should be accompanied by the reasons for the delay and information can be provided in phases without further undue delay. Where such delay is justified, less sensitive or less specific information on the breach should be released as early as possible, rather than fully resolving the underlying incident before notifying.

- The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close co-operation with the Data Protection Officer, respecting guidance provided by him or her or by other relevant authorities such as law-enforcement authorities.

O. TRANSITIONAL REGIME

36. The new data protection framework will bring significant improvements to the EPO's data protection system. In order to give the Office and its users, partners and other stakeholders sufficient time to adapt to the new rules and requirements, a staged transition is proposed:

37. It is envisaged that the new data protection framework will enter into force on 1 January 2022. This implies a first six-month transition period from the date of adoption by the Administrative Council until entry into force. Once the new framework enters into force, it will apply only to data processing operations that are ongoing or initiated on or after 1 January 2022.

38. A second six-month transition period then ensues during which the Office can bring data processing operations which were ongoing prior to the adoption of the new DPR into line with the new framework. In exceptional circumstances, this period may be further extended by the DPO.

VI. ALTERNATIVES

39. N/A

VII. FINANCIAL IMPLICATIONS

40. The implementation of this proposal on the revised DPR is not expected to generate major costs for the Office.

VIII. LEGAL BASIS

41. Article 33(2)(b) EPC.

IX. DOCUMENTS CITED

42. CA/65/19

X. RECOMMENDATION FOR PUBLICATION

43. Yes.

PART II

Draft

DECISION OF THE ADMINISTRATIVE COUNCIL
of [date of decision]
introducing a new data protection framework at the European Patent Office

---

THE ADMINISTRATIVE COUNCIL OF THE EUROPEAN PATENT ORGANISATION,

Having regard to the European Patent Convention and in particular Articles 10(2)(c) and 33(2)(b) thereof,

Having regard to the Service Regulations for permanent and other employees of the European Patent Office (hereinafter referred to as "the Service Regulations"),

Having regard to the Guidelines for the Protection of Personal Data in the European Patent Office,

Having regard to the organisational autonomy and judicial independence of the Boards of Appeal,

On a proposal from the President of the European Patent Office, submitted after consulting the General Consultative Committee and the President of the Boards of Appeal,

HAS DECIDED AS FOLLOWS:

I. Amendments to the Service Regulations

Article 1

Article 2(1) of the Service Regulations shall read as follows (addition underlined):

"(1) There shall be set up within the Office:

(a) a Staff Committee,

(b) a General Consultative Committee,

(c) Disciplinary Committees,

(d) an Appeals Committee,

(e) Occupational Health, Safety and Ergonomics Committees,

(f) an Appraisals Committee,

(g) a Joint Committee on Articles 52 and 53,

(h) a Data Protection Board

which shall perform the functions assigned to them under these Service Regulations."

Article 2

Article 109(3) of the Service Regulations shall read as follows (addition underlined):

"(3) Appraisal reports referred to in Article 47a and individual decisions taken under Articles 49 and 50 of the Implementing Rules for Articles 1b and 32a shall be excluded from the review procedure."

Article 3

Article 110(2) of the Service Regulations shall read as follows (addition underlined):

"(2) The following individual decisions are excluded from the internal appeal procedure:

(a) Individual decisions taken on requests to carry on working after reaching the age of sixty-five under Article 54, paragraph 1;

(b) individual decisions taken after consultation of the Disciplinary Committee in accordance with Article 103;

(c) individual decisions taken after consultation of the Joint Committee in accordance with Article 53b, paragraph 4;

(d) individual decisions taken on requests to perform duties at a location other than the Office's premises pursuant to Article 55a and any implementing instructions thereto;

(e) appraisal reports referred to in Article 47a;

(f) individual decisions taken under Articles 49 and 50 of the Implementing Rules for Articles 1b and 32a."

Article 4

The following new Article 1b shall be inserted into the Service Regulations:

"**Article 1b**

Protection of personal data

(1) 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.

(2) This Article, Article 32a and their Implementing Rules shall apply to the Office's processing of personal data wholly or partly by automated means and to its processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system; in applying them, due regard shall be had to the independence of the Boards of Appeal in their judicial capacity. The scope of this Article, Article 32a and their Implementing Rules shall extend to all natural persons not covered by Article 1 whose personal data are processed by the Office.

(3) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection, as the context of their processing could create significant risks to those fundamental rights and freedoms. Such personal data shall not be processed unless the specific conditions set out in the Implementing Rules for Articles 1b and 32a are met. Those personal data may include personal data revealing racial or ethnic origin; the use of the terms "race" and "racial origin" in these Service Regulations and their Implementing Rules is not, however, to be construed as implying an acceptance by the European Patent Organisation of theories which attempt to determine the existence of separate human races.

(4) The Office shall endeavour to put in place measures which facilitate the exercise of the data subject's rights under these Service Regulations and their Implementing Rules, including mechanisms for requesting and, if applicable, obtaining free of charge, in particular, access to and rectification or erasure of personal data and for exercising the right to object.

(5) Where personal data might lawfully be processed because processing is necessary to carry out tasks in the exercise of the official activities of the European Patent Organisation 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, a data subject shall nevertheless be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject."

Article 5

The following new Article 32a shall be inserted into the Service Regulations:

"**Article 32a**

Data protection oversight mechanisms

(1) The Data Protection Officer shall monitor the application of the provisions on the protection of personal data and advise the various operational units of the Office on fulfilling their obligations. The Data Protection Officer shall provide the operational units with the operational documentation necessary for the practical implementation of this Article and its Implementing Rules, such as workflows, handbooks, forms and templates.

(2) The Data Protection Board shall oversee that the fundamental rights and freedoms of natural persons, including their right to data protection, are respected in the application of the provisions on the protection of personal data. For this purpose, it shall provide independent, effective and impartial oversight of the provisions applicable to the protection of personal data.

(3) The Office shall offer data subjects effective and timely redress mechanisms with the aim of ensuring compliance with data protection requirements and the rights of the data subjects, which include effective legal redress and the right to claim compensation.

(4) The Data Protection Officer and any deputy shall act completely independently of any internal or external interference in performing their tasks and exercising their powers.

(5) The Data Protection Board shall act completely independently of any internal or external interference in performing its tasks and exercising its powers.

(6) The Data Protection Officer shall report regularly to the Administrative Council on the implementation of the Office's data protection framework.

(7) For the purposes of processing personal data in their judicial capacity, the Boards of Appeal may deviate from the above provisions in accordance with independent oversight mechanism rules."

II. New Implementing Rules for Articles 1b (Protection of personal data) and 32a (Data protection oversight mechanisms) of the Service Regulations for permanent and other employees of the European Patent Office

Article 6

The Implementing Rules for Articles 1b and 32a (Protection of personal data and data protection oversight mechanisms) of the Service Regulations for permanent and other employees of the European Patent Office set out in Annex 1 to this decision are adopted.

III. Entry into force

Article 7

This decision shall enter into force on 1 January 2022.

Done at Munich, [date of decision]

For the Administrative Council
The Chairman

Josef KRATOCHVÍL

Annex 1: Implementing Rules for Articles 1b and 32a of the Service Regulations (Protection of personal data and data protection oversight mechanisms)

ANNEX 1

**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**

TABLE OF CONTENTS

These Implementing Rules set out the principles and detailed provisions governing the processing of personal data under Articles 1b and 32a of the Service Regulations.

I. General provisions

Article 1
Purpose

(1) The purpose of these Rules is to support the implementation of Articles 1b and 32a of the Service Regulations by establishing 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 and to provide for accountability in this regard.

(2) These Rules will be supplemented by

(a) further rules, administrative instructions and decisions adopted by the President of the Office,

(b) administrative instructions adopted by the President of the Boards of Appeal in the context of the powers under Articles 10(2)(a), (e), (f) and (h), 11(3) and (5) and 48(1) of the European Patent Convention (EPC) which have been delegated to him or her by the President of the Office in so far as they relate to the Boards of Appeal Unit and its staff, including the members and Chairs of the Boards of Appeal and of the Enlarged Board of Appeal (Act of Delegation), and

(c) operational documents issued by the Data Protection Officer, which will specify more detailed requirements and procedures for the processing of personal data.

Article 2
Field of application

(1) These Rules apply to the Office's processing of personal data wholly or partly by automated means and to its processing other than by automated means of personal data which form or are intended to form part of a filing system.

(2) These Rules apply to all persons covered by Article 1 of the Service Regulations.

(3) These Rules also apply to all natural persons not covered by paragraph 2 whose personal data are processed by the Office.

(4) These Rules do not apply to the processing of personal data of deceased persons, of personal data which concerns legal persons or of anonymous information.

(5) Files or sets of files, including their cover pages, which are not structured according to specific criteria do not fall within the scope of these Rules.

(6) Articles 49 to 52 do not apply to the processing of personal data by the Boards of Appeal in their judicial capacity. An independent oversight mechanism for the Boards of Appeal shall be established to ensure compliance with these Rules.

Article 3
Definitions

(1) For the purposes of these Rules:

a. "**personal data**" means any information relating to any identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity; personal data which have undergone pseudonymisation but which could be attributed to a natural person by the use of additional information are to be considered to be information relating to an identifiable natural person.

b. "**processing**" of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

c. "**restriction of processing**" means the marking of stored personal data with the aim of limiting their processing in the future, including programming measures to permanently prevent access to such data.

d. "**profiling**" means 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.

e. "**pseudonymisation**" means 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.
f. "**filing system**" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
g. "**controller**" means the entity, namely the European Patent Office, which, alone or jointly with others, determines the purposes and means of the processing of personal data.
h. "**delegated controller**" means the operational unit, represented by its head, ensuring that all processing operations involving personal data that are performed within the operational unit comply with these Rules. The person representing the unit shall be a manager at senior level, normally at least a principal director.
i. "**operational unit**" means an organisational unit of the Office performing tasks and/or activities within the Office and defining the purpose, rationale and business needs of a processing operation.
j. "**processor**" means a natural or legal person, public authority, agency or any other entity which processes personal data on behalf of the controller.
k. "**recipient**" means a natural or legal person, public authority, agency or any other entity to which personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data within the framework of a particular inquiry in accordance with the Protocol on Privileges and Immunities of the European Patent Organisation are not to be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the data protection rules applicable in view of the purposes of the processing.
l. "**third party**" means 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.
m. "**consent**" of the data subject means 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.
n. "**personal data breach**" means 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.
o. "**genetic data**" means 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.
p. "**biometric data**" means 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. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through specific technical means allowing the unique identification or authentication of a natural person.
q. "**personal data concerning health**" means 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.
r. "**anonymous information**" means 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.
s. "**transmission of personal data**" means disclosure, dissemination of or otherwise making available, including by granting access, of personal data to a party within the European Patent Organisation or to a national industrial property office or other public authority of a contracting state to the European Patent Convention under the conditions laid down in Article 8.
t. "**transfer of personal data**" means disclosure, dissemination of or otherwise making available, including by granting access, of personal data to a person or an entity outside the European Patent Organisation which is neither a national industrial property office nor a public authority of a contracting state to the European Patent Convention under the conditions laid down in Article 9.
u. "**third country**" means a country which is not a contracting state to the European Patent Convention.
v. "**erasure of data**" means the obliteration of stored data in such a way that reconstruction is not possible.
w. "**data subject**" means any identified or identifiable natural person, irrespective of whether that person is an employee of the Office or not; to determine whether a natural person is identifiable, account should 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.
x. "**employee**" means every person covered by Article 1 of the Service Regulations.
y. "**legal provisions of the European Patent Organisation**" means the European Patent Convention or its constituent parts, international agreements and other legal arrangements concluded by the President of the Office, rules and instruments enacted by the Administrative Council, as well as circulars, communiqués and all other legal provisions adopted or issued by the President of the Office or by the President of the Boards of Appeal.

z. "**information society service**" means any service provided at a distance, by electronic means and at the individual request of a recipient of services.

II. General rules on the lawfulness of processing personal data

Article 4
Principles relating to processing of personal data

(1) The controller ensures that the principles set out in this Article are observed. In particular, the controller is responsible for, and shall be able to demonstrate, compliance with paragraph 2 ("accountability"). The controller shall ensure that the processing of personal data, including the reasons for it and the means used, is appropriately documented. To this end, the controller shall follow a structured and risk-based approach to designing and documenting processing operations. The controller shall 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. Due regard shall be had to the organisational autonomy of the Boards of Appeal Unit and to the judicial independence of the Boards of Appeal.

(2) Personal data shall be:

a. processed lawfully, fairly and in a manner transparent to the data subject ("lawfulness, fairness and transparency"); the data subject shall be informed of the existence of the processing operation and its purposes, and the controller shall provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed;
b. collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with these purposes ("purpose limitation");
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
d. accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that personal data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified without delay ("accuracy");
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data were collected or for which they are further processed ("storage limitation");
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

(3) As a general rule, personal data shall be collected from the data subject wherever possible.

Article 5
Lawfulness of processing

Processing of personal data is lawful only if and to the extent that at least one of the following applies:

a. processing is necessary for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation 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, or
b. processing is necessary for compliance with a legal obligation to which the controller is subject, or
c. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or
d. the data subject has given explicit consent to the processing of his or her personal data for one or more specific purposes, or
e. processing is necessary in order to protect the vital interests of the data subject or of another natural person.

Article 6
Processing for another compatible purpose

(1) Without prejudice to Articles 4, 6 and 12, the controller may process personal data for a purpose other than that for which the personal data were collected only if such other purpose is compatible with the purpose for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. The legal basis for the initial collection and processing of personal data provided by the applicable legal provisions of the European Patent Organisation may also serve as a legal basis for further processing. However, data may not be further processed in a way that is unexpected, inappropriate or objectionable for the data subject.

(2) Personal data may also be processed for purposes other than those for which they have been collected, if such processing can be based on the data subject's explicit consent or applicable legal provisions of the European Patent Organisation which constitute a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 25.

(3) Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's explicit consent or on applicable legal provisions of the European Patent Organisation, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purposes for which the personal data were initially collected, take into account, inter alia:

a. any link between the purposes for which the personal data were collected and the purpose of the intended further processing;
b. the context in which the personal data were collected, in particular regarding the relationship between data subjects and the controller;
c. the nature of the personal data, in particular whether special categories of personal data are processed pursuant to Article 11 or whether personal data related to criminal convictions and offences are processed pursuant to Article 12;
d. the possible consequences of the intended further processing for data subjects;
e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7
Conditions for consent

(1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

(2) Consent shall be given by a clear and affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, for example in the form of a written statement, including one made by electronic means, or an oral statement.

(3) Consent shall cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent shall be given for each one of them.

(4) For consent to be informed, the data subject shall be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. 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.

(5) The data subject shall have the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed of this. It shall be as easy to withdraw as to give consent. In order to ensure that consent is freely given, consent cannot provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and it is therefore unlikely in view of all the circumstances of that specific situation that consent was freely given.

(6) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of these Rules will not be binding.

(7) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

(8) Where Article 5(d) applies in relation to the offer of information society services directly to a child, the processing of the child's personal data is lawful where the child is at least 13 years old. Where the child is below the age of 13, such processing is lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

Article 8
Transmission of personal data to public authorities within the territory of the contracting states and to a national industrial property office of a contracting state

(1) Without prejudice to Articles 4, 5, 6, 11 and 12, personal data may be transmitted from the Office to a recipient outside the Office but within the territory of the contracting states only if the recipient is a public authority and the data are necessary for the performance of tasks within the recipient's competence and where the transmission is compatible with the tasks and the functioning of the Office.

(2) Without prejudice to Articles 4, 5, 6, 11 and 12, personal data may be transmitted by the Office to a national industrial property office of a contracting state if the data are necessary for the performance of tasks within the recipient's competence or for the exercise of the official authority vested in it and processing is necessary to carry out tasks in the exercise of the official activities of the European Patent Organisation 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.

(3) The recipient shall provide evidence that it is necessary to have the data transmitted for a specific purpose deriving from the Office's obligations of co-operation with the contracting states. The controller, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, shall establish that it is proportionate to transmit the personal data for that specific purpose, after having demonstrably weighed up the various competing interests.

(4) Where the controller initiates a transmission under paragraph 1 or 2, it shall demonstrate that the transmission of personal data is necessary for and proportionate to the purposes of the transmission by applying the criteria laid down in those paragraphs.

(5) Without prejudice to Articles 4, 5, 6, 11 and 12, where the processing is to be carried out by a private entity engaged on behalf of the controller, personal data may be transmitted from the Office within the territory of the European Economic Area only if in compliance with these Rules and under the conditions set forth in Articles 30 and 31 of these Rules.

Article 9
Transfer of personal data

(1) Transfers of personal data shall take place only if in compliance with these Rules, including the conditions laid down in this Article and/or Article 10. This also applies to transfers of data intended for processing after transfer to a third country or to an international organisation, and to onward transfers of personal data from a third country or an international organisation to another third country or to another international organisation. All provisions in this Article and/or Article 10 shall be applied in order to ensure that the level of protection of natural persons guaranteed by these Rules is not undermined.

(2) The transfer of personal data to recipients outside the European Patent Office which are not covered by Article 8(1), (2) and (5) is permissible only if an adequate level of protection is ensured in the country of the recipient, or in a territory or one or more sectors within that country, or within the receiving international organisation and the data are transferred solely to allow tasks within the competence of the controller to be carried out.

(3) In cases of doubt, the President of the Office decides, after consulting the Data Protection Officer and the Data Protection Board, whether the protection afforded by the country or international organisation in question can be considered adequate.

(4) Transfers outside the European Patent Office to recipients which are not covered by Article 8(1) and (2) may be carried out to public authorities or bodies in third countries, or to international organisations with corresponding duties or functions on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects.

(5) In the absence of an adequate level of protection pursuant to paragraphs 1 and 3, the controller or processor may transfer personal data to recipients outside the European Patent Office only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such appropriate safeguards may be provided for by appropriate contractual clauses drafted after consultation of the Data Protection Board or by appropriate certification mechanisms.

(6) Personal data transferred under this Article may be processed or used only for the purpose for which they have been transferred. They shall be deleted as soon as that purpose has been achieved. The recipient shall be advised of this and obliged to act accordingly by contract or agreement. The recipient shall provide evidence that it is necessary to have the data transferred for a specific purpose. The controller, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, shall establish that it is proportionate to transfer the personal data for that specific purpose after having demonstrably weighed up the various competing interests.

(7) Where the controller initiates a transfer of personal data under this Article, it shall demonstrate that this transfer is necessary for and proportionate to the purposes of the transfer by applying the criteria laid down in this Article.

Article 10
Derogations for specific situations

(1) In the absence of an adequate level of protection in the country of the recipient, or of appropriate safeguards under Article 9, the transfer of personal data to recipients outside the European Patent Office which are not a national industrial property office of a contracting state is permissible only exceptionally where:

a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequate level of protection and appropriate safeguards;
b. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for the performance of a task in the exercise of the official activities of the European Patent Organisation 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, or to perform obligations arising from its duty of co-operation with the contracting states;
e. the data transfer is necessary for the establishment, exercise or defence of legal claims and their transmission is not precluded by agreements under international law or other applicable legal provisions of the European Patent Organisation;
f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving explicit consent; or
g. the transfer is made from a register which, according to the legal provisions of the European Patent Organisation, is 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 case.

(2) Provision should be made in specific situations for the possibility of transfers in certain circumstances where the data subject has given his or her explicit consent and where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure. Provision should also be made for the possibility of transfers where required to perform obligations arising from the Office's duty of co-operation with the contracting states or where the transfer is made from a register established by the legal provisions of the European Patent Organisation and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should 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.

(3) Paragraph 1(a), (b) and (c) does not apply to tasks carried out by the European Patent Office in the exercise of its official activities.

(4) What constitutes a task carried out in the exercise of the official activities of the European Patent Office 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, or an obligation arising from the Office's duty of co-operation with the contracting states referred to in paragraph 1(d) is to be established on the basis of the European Patent Convention and/or other applicable legal provisions of the European Patent Organisation.

(5) A transfer pursuant to paragraph 1(g) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register, unless authorised by the applicable legal provisions of the European Patent Organisation. Where the register is intended for consultation by persons having a legitimate interest, the transfer may 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.

(6) These derogations shall apply in particular to data transfers required and necessary in the exercise of the official activities of the European Patent Organisation or the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office's management and functioning, or in reason of obligations deriving from its duty of co-operation with the contracting states, for example in cases of international data exchange 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. A transfer of personal data is also to be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving explicit consent. In the absence of an adequacy decision within the meaning of Article 9(2), the President of the Office may, in accordance with Article 9(4), and for important reasons relating to the legitimate exercise of the official authority vested in the Office, which 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, expressly set limits to the transfer of specific categories of data to a third country or an international organisation.

Article 11
Processing of special categories of personal data

(1) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, of genetic data or biometric data for the purpose of uniquely identifying a natural person and of data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited.

(2) Paragraph 1 does not apply where one of the following applies:

a. the data subject has given explicit consent to the processing of those data for one or more specified purposes.
b. processing 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 in so far as it is authorised by legal provisions of the European Patent Organisation providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
c. processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving explicit consent.
d. processing relates to personal data which have been manifestly made public by the data subject.
e. the processing is necessary for the establishment, exercise or defence of legal claims.
f. the processing is necessary for a specific purpose relating to the performance of a task carried out in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing substantially necessary for the management and functioning of the Office, having regard to the principle of proportionality, or in reason of obligations arising from its duty of co-operation with the contracting states. This processing shall be based on a legal instrument which is 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.
g. the processing is 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 measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

(3) Paragraph 1 does not apply where processing of the special categories of data is required for the purposes of 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 provided for in the Service Regulations or other legal provisions of the European Patent Organisation and 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 12
Processing of personal data relating to criminal convictions and offences

(1) Processing of data relating to criminal offences, criminal convictions or security measures based on Article 5(a) may be carried out only after consultation of the Data Protection Board or when the processing is covered by legal provisions of the European Patent Organisation providing for appropriate safeguards for the rights and freedoms of data subjects.

(2) Suspicions regarding offences shall also be included in the concept of "offences", since the processing of data relating to matters which have not led to convictions requires protection equal to that afforded to criminal convictions.

(3) The term "security measures" under this Article refers to measures taken against individuals in the context of a criminal (or administrative) procedure, such as forced admission to a psychiatric hospital or asset freezes.

Article 13
Processing which does not require identification

(1) If the purposes for which the controller processes personal data do not or no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with these Rules.

(2) Where, in cases referred to in paragraph 1, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 18 to 22 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification. The controller shall not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights.

Article 14
Safeguards relating to processing for archiving purposes in the legitimate exercise of the official authority vested in the controller, scientific or historical research purposes or statistical purposes

Processing for archiving purposes in the legitimate exercise of the official authority vested in the controller, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with these Rules, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

III. Rights of the data subject

Article 15
Transparency and modalities for the exercise of the rights of the data subject

(1) The controller shall take appropriate measures to provide the data subject with any information referred to in Articles 16 and 17 and any communication referred to in Articles 18 to 24 and Article 34 relating to processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information is to be provided in writing or by other means, including, where appropriate, electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

(2) The controller shall facilitate the exercise of data subject rights under Articles 18 to 24. The controller shall provide data subjects with information on measures taken on a request under Articles 18 to 24 without undue delay and in any event within one month of receipt of the request. The controller, acting in consultation with the Data Protection Officer, may extend that period by two further months where necessary in view of the complexity and number of requests. If such an extension of the standard time limit is needed, the controller shall duly notify the data subject of the extension and the reasons for the delay within one month of the Office's receipt of the request. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(3) If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and of the possibility of filing a request for review and seeking legal redress under Articles 49 and 50.

(4) Information provided under Articles 16 and 17 and any communication issued and actions taken under Articles 18 to 24 and 34 shall be free of charge. 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.

(5) Where the controller has reasonable doubts concerning the identity of the natural person making a request under Articles 18 to 24, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

(6) The information to be provided to data subjects pursuant to Articles 16 and 17 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically, they shall be machine-readable.

Article 16
Information to be provided where personal data are collected from the data subject

(1) Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

a. the identity and the contact details of the controller;
b. the contact details of the Data Protection Officer;
c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d. the recipients or categories of recipients of the personal data, if any;
e. where applicable, the fact that the controller intends to transfer personal data to recipients under Article 9 and reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a. the period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period;
b. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;
c. where the processing is based on Article 5(d) or Article 11(2)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d. the right to request review by the delegated controller under Article 49 and the right to seek legal redress under Article 50;
e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of a failure to provide such data;
f. the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) Where the delegated controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the delegated controller shall provide the data subject with information on that other purpose and with any relevant further information referred to in paragraph 2 prior to that further processing.

(4) Paragraphs 1, 2 and 3 do not apply where and in so far as the data subject already has the information.

Article 17
Information to be provided where personal data have not been obtained from the data subject

(1) Where personal data have not been obtained from the data subject, the controller shall, at the time when personal data are obtained and in addition to the information to be provided under Article 16, provide the data subject with information on the categories of personal data concerned and the source of the personal data and, if applicable, whether they came from publicly accessible sources.

(2) In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing in respect of the data subject:

a. the period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period;
b. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or, where applicable, the right to object to processing or the right to data portability;
c. where the processing is based on Article 5(d) or Article 11(2)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d. the right to request review by the delegated controller under Article 49 and the right to seek legal redress under Article 50;
e. from which source the personal data originate, and if applicable, whether they came from publicly accessible sources;
f. the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) The controller shall provide the data subject with the information referred to in paragraphs 1 and 2:

a. within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed,
b. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject, or
c. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

(4) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

(5) Paragraphs 1 to 4 shall not apply where and insofar as:

a. the data subject already has the information;
b. the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the legitimate exercise of the official authority vested in the controller, scientific or historical research purposes or statistical purposes or in so far as the obligation referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing;
c. obtaining or disclosure is expressly laid down in the European Patent Convention and/or other applicable legal provisions of the European Patent Organisation which provide appropriate measures to protect the data subject's legitimate interests; or
d. the personal data must remain confidential subject to an obligation of professional secrecy regulated on the basis of the European Patent Convention and/or other applicable legal provisions of the European Patent Organisation, including a statutory obligation of secrecy.

Article 18
Rights of access by the data subjects

(1) The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, if so, to access the personal data easily and at reasonable intervals, to understand which data about him or her are processed, to verify the quality of his or her personal data, to verify the lawfulness of their processing and to exercise his or her other data protection rights and be provided with the following information:

a. the purposes of the processing;
b. the categories of personal data concerned;
c. the recipients or categories of recipient to which the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d. where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period;
e. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f. the right to request review by the delegated controller under Article 49 and to seek legal redress under Article 50;
g. where the personal data are not collected from the data subject, any available information as to their source;
h. the existence of automated decision-making, including profiling referred to in Article 24(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred in accordance with Article 9, the data subject has the right to be informed of the appropriate safeguards pursuant to the same Article put in place for the transfer.

(3) The right of the data subject to access his or her own personal data does not entitle the data subject to an indiscriminate right to access all documents. The controller shall grant access to the data subject to the fullest extent possible unless a restriction under Article 25 applies. The controller shall 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)). If necessary to safeguard the confidentiality of the Office's deliberations and decision-making, certain information may be deleted from the copy provided to the data subject. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(4) Where the controller processes a large quantity of information concerning the data subject, the controller is able to request that, before the information is delivered, the data subject specifies the information or processing activities to which the request relates.

(5) The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Article 19
Right to rectification

(1) The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

(2) The right of rectification only applies to objective and factual data, e.g. identification data, which can be rectified at any time during a procedure or identification data linked to an administrative management system. It does not apply to subjective statements, including those made by third parties. However, in such cases, the data subject shall be permitted to complement existing data with a second opinion or counter-expertise or to provide comments.

(3) The controller shall communicate any rectification of personal data carried out in accordance with paragraph 1 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20
Right to erasure ("right to be forgotten")

(1) The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller is obliged to erase personal data without undue delay where one of the following grounds applies:

a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b. the data subject withdraws the consent on which the processing is based under Article 5(d) or Article 11(2)(a) and there is no other legal ground for the processing;
c. the data subject objects to the processing pursuant to Article 23(1) and there are no overriding legitimate grounds for the processing;
d. the personal data were unlawfully processed;
e. the personal data have to be erased for compliance with a legal obligation to which the controller is subject;
f. the personal data have been collected in relation to the offer of information society services referred to in Article 7(8).

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 do not apply to the extent that processing is necessary:

a. for exercising the right of freedom of expression and information;
b. for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in reason of obligations arising from the Office's duty of co-operation with the contracting states or in the exercise of official authority vested in the controller;

c. for reasons of co-operation with the contracting states in the area of public health in accordance with Article 11;
d. for archiving purposes in the legitimate exercise of the official activities of the European Patent Organisation, or of the official authority vested in the controller, which includes the processing necessary for its management and functioning, for scientific or historical research purposes or statistical purposes, in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e. for the establishment, exercise or defence of legal claims.

(4) The controller shall communicate any erasure of personal data carried out in accordance with paragraph 1 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 21
Right to restriction of processing

(1) The data subject has the right to obtain from the controller restriction of processing where one of the following applies:

a. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the personal data;
b. the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
d. the data subject has objected to processing pursuant Article 23(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing has been restricted under paragraph 1, the personal data may, with the exception of storage, only be processed with the data subject's explicit consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation 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.

(3) A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

(4) In automated filing systems restriction of processing shall as a rule be ensured by technical means. The fact that the processing of the personal data is restricted shall be indicated in the system in such a way that it is clear that the personal data shall not be used.

(5) The controller shall communicate any restriction of processing carried out in accordance with paragraphs 1 to 4 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 22
Right to data portability

(1) The data subject has the right to receive, in a structured, commonly used and machine-readable format, the personal data concerning him or her which he or she has provided to the controller and the right to transmit those data to another controller without hindrance from the controller to which the personal data were initially provided where:

a. the processing is based on consent pursuant to Article 5(d) or Article 11(2)(a) or on a contract pursuant to Article 5(c); and
b. the processing is carried out by automated means.

(2) In exercising his or her right to data portability pursuant to paragraph 1, the data subject has the right to have the personal data transmitted directly from one controller to another where technically feasible.

(3) The exercise of the right referred to in paragraph 1 is without prejudice to Article 20. That right does not apply to processing 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 management and functioning of the Office.

(4) The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Article 23
The right of the data subject to object

(1) The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on Article 5(a), including profiling based on that provision. The controller shall cease to process the personal data unless the controller demonstrates 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.

(2) At the latest at the time of the first communication with the data subject, the right referred to in paragraph 1 shall be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(3) Without prejudice to Articles 35 and 36, in the context of the use of information society services the data subject may exercise his or her right to object by automated means using technical specifications.

(4) Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject has the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her 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 24
Automated individual decision-making, including profiling

(1) The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or similarly significantly affecting him or her.

(2) Paragraph 1 does not apply if the decision:

a. is necessary for entering into, or performance of, a contract between the data subject and the controller;
b. is authorised by a legal act adopted on the basis of the European Patent Convention or other applicable legal provisions of the European Patent Organisation and also laying down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
c. is based on the data subject's explicit consent.

(3) In the cases referred to in paragraph 2(a) and (c), the controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

(4) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 11(1), unless Article 11(2)(a) or (f) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 25
Restriction of rights

(1) Specific legal provisions may restrict the application of Articles 15 to 22, 34 and 35, as well as of Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 15 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

a. the European Patent Organisation's security, public security or defence of the contracting states;
b. 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 and including cases in which Article 20 of the Protocol of Privileges and Immunities is applied;
c. other substantial interests of the European Patent Organisation 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;

d. the internal security of the Office, including of its electronic communications networks;
e. the protection of judicial and quasi-judicial independence and judicial and quasi-judicial proceedings;
f. the prevention, investigation, detection and sanction of breaches of ethics for regulated professions;
g. a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority;
h. the protection of the data subject or the rights and freedoms of others;
i. the enforcement of civil law claims.

(2) In particular, any such specific legal provision of the European Patent Organisation within the meaning of paragraph 1 shall contain specific provisions, where relevant, as to:

a. the purposes of the processing or categories of processing;
b. the categories of personal data;
c. the scope of the restrictions introduced;
d. the safeguards to prevent abuse or unlawful access or transfer;
e. the specification of the controller or categories of controllers;
f. the storage periods and the applicable safeguards, taking into account the nature, scope and purposes of the processing or categories of processing; and
g. the risks to the rights and freedoms of data subjects.

(3) The restrictions are subject to following limits:

a. The provisions on the basis of which the restrictions referred to in paragraph 1 take place shall be clear and precise and intended to produce legal effects vis-à-vis data subjects. They shall be adopted at least at the level of the President of the Office. When the President of the Boards of Appeal is the controller, they shall be adopted at least at the level of the President of the Boards of Appeal. In both cases, they shall be submitted to the Administrative Council for information. On the basis of these provisions, each time a delegated controller needs to impose a restriction it shall first carry out a duly documented "necessity and proportionality test". The Data Protection Officer shall be involved in the "proportionality and necessity test assessment note" and the subsequent reviews and shall keep a register listing all decisions allowing delegated controllers to apply restrictions.
b. If a restriction is imposed pursuant to paragraph 1, the data subject shall be informed of the principal reasons on which the application of the restriction is based and of his or her right to submit a request to the Data Protection Officer under Article 43(2) and/or of the possibility of filing a request for review by the delegated controller and seeking legal redress under Articles 49 and 50.
c. If a restriction imposed pursuant to paragraph 1 is relied upon to deny access to the data subject, the Data Protection Officer and/or the entities involved in the request for review by the delegated controller and in the proceedings for legal redress shall, when investigating the request, only inform him or her whether the data have been processed correctly and, if not, whether any necessary corrections have been made.

(4) Provision of the information referred to in paragraphs 3(b) and (c) and in Article 43(2) may be deferred, omitted or denied if it would cancel the effect of the restriction imposed pursuant to paragraph 1.

IV. Controller and processor

Article 26
Responsibility of the controller

(1) Taking into account the nature, scope, context and purposes of processing and the varying likelihood and severity of any risks for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with these Rules. Those measures shall be reviewed and updated where necessary.

(2) Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

(3) Adherence to approved certification mechanisms may serve as evidence of compliance with the obligations of the controller.

Article 27
Data protection by design and by default

(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing and the varying likelihood and severity of any risks for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself ("by design"), implement appropriate technical and organisational measures which are designed to implement the data protection principles outlined in Article 4 and to integrate the necessary safeguards into the processing in order to meet the requirements of these Rules.

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that, by default, personal data are not made accessible to an indefinite number of natural persons without the individual's intervention.

(3) A certification mechanism may serve as evidence of compliance with the requirements set out in paragraphs 1 and 2.

Article 28
Controller and delegated controllers

(1) The President of the Office acts as the controller of the personal data processed by the Office, unless otherwise specified.

(2) The President of the Boards of Appeal acts as the controller with regard to the personal data processing operations carried out as part of the judicial activity of the Boards of Appeal and in the exercise of functions and powers under the Act of Delegation. With regard to the personal data processing operations carried out by the Boards of Appeal Unit in the context of all other activities, the President of the Boards of Appeal acts as a delegated controller.

(3) The controller is free to delegate the competence of determining the purposes and means of processing certain personal data to an operational unit.

(4) Delegated controllers may not sub-delegate the controllership unless a specific unit's functional independence might otherwise be jeopardised or its size exceptionally requires a sub-delegation to a lower hierarchical level and the Data Protection Officer authorises it. The requisite act of sub-delegation or its withdrawal is valid only if the Data Protection Officer has been notified of it.

Article 29
Joint controllers

(1) Where the controller together with one or more controllers outside the Office jointly determine the purposes and means of processing, they will be joint controllers. Joint controllers shall determine, in a transparent manner, their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 16 to 24, by means of an arrangement between them. The arrangement may designate a contact point for data subjects.

(2) The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject as further specified in the operational documents.

(3) Irrespective of the terms of the arrangement referred to in paragraph 2, the data subject may request exercise of his or her rights under these Rules in respect of, and enforce these rights against, each of the controllers.

Article 30
Processor

(1) Where processing is to be carried out on behalf of the controller, the controller shall use only processors providing sufficient guarantees that appropriate technical and organisational measures will be implemented in such a manner that processing will meet the requirements of these Rules and ensure the protection of the rights of the data subject.

(2) The processor shall not engage another processor without prior specific or general written authorisation from the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(3) Processing by a processor shall be governed by a contract or legal act, adopted on the basis of the applicable legal provisions of the European Patent Organisation, which is binding on the processor with regard to the controller and sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

a. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by the law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
b. ensures that persons authorised to process the personal data have undertaken to maintain confidentiality or are under an appropriate statutory obligation of confidentiality;
c. takes all appropriate technical and organisational measures to ensure a level of security appropriate to the risk;
d. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
e. taking into account the nature of the processing, assists the controller, as far as possible, by appropriate technical and organisational measures to fulfil the controller's obligation to respond to requests for exercising the data subject's rights laid down in these Rules;
f. assists the controller in ensuring compliance with its obligations, taking into account the nature of processing and the information available to the processor;
g. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the applicable law requires storage of the personal data and the Office agrees to such storage;
h. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) above, the processor shall immediately inform the controller if, in its opinion, an instruction infringes these Rules.

(4) Where a processor engages another processor to carry out specific processing activities on behalf of the controller, the same data protection obligations as set out in the legal act or contract between the controller and the processor referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal instrument, in particular as regards providing sufficient guarantees that appropriate technical and organisational measures will be implemented in such a manner that the processing will meet the requirements of these Rules. Where that other processor fails to fulfil its data protection obligations, the initial processor will remain fully liable to the controller for the performance of that other processor's obligations.

(5) Adherence of the processor to an approved code of conduct or an approved certification mechanism may serve as evidence of sufficient guarantees as referred to in paragraphs 1 and 4. A list of the codes of conducts and certification mechanisms approved by the Office will be published.

(6) Without prejudice to any individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8, including when they are part of a certification granted to the processor.

(7) The Office may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 or approve standard contractual clauses adopted by other institutions.

(8) The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, which may also take electronic form.

(9) Without prejudice to Article 52, if a processor infringes these Rules by determining the purposes and means of processing, the processor will be considered to be a controller in respect of that processing.

Article 31
Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or the processor who has access to personal data shall not process those data except on instructions from the controller, unless required to do so by the law to which the processor is subject.

Article 32
Records of processing activities

(1) Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

a. the name and contact details of the controller and/or the delegated controller, the Data Protection Officer and, where applicable, the processor and the joint controller;
b. the purposes of the processing;
c. a description of the categories of data subjects and of the categories of personal data;
d. the categories of recipients to which the personal data have been or will be disclosed, including recipients in third countries or other international organisations;
e. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
f. where possible, the envisaged time limits for erasure of the different categories of data;
g. where possible, a general description of the technical and organisational security measures referred to in Article 33.

(2) Each processor shall maintain a record of all categories of processing activities carried out on behalf of the controller which contains:

a. the names and contact details of the processor or processors, each controller on behalf of which the processor is acting and the Data Protection Officer;
b. the categories of processing carried out on behalf of each controller;
c. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
d. where possible, a general description of the technical and organisational security measures referred to in Article 33.

(3) The records referred to in paragraphs 1 and 2 shall be in writing, which may also take electronic form.

(4) The Office shall make its records available to the Data Protection Board on request.

(5) The Office's records of processing activities will be kept in a central register.

(6) The central register will be made publicly accessible, save for any confidential records.

V. Confidentiality and security of processing

Article 33
Confidentiality and security of processing

(1) 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 natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, as appropriate:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2) In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

(3) The controller and processor shall take steps to ensure that any natural person acting on behalf of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless required to do so by the law to which he or she is subject. This exemption does not apply to persons covered by Article 1 of the Service Regulations.

(4) Specific requirements as to data security will be laid down in the operational documents. Adherence to an approved certification mechanism may serve as evidence of compliance with the requirements set out in paragraph 1.

Article 34
Notification and communication of a personal data breach

(1) In the case of a personal data breach, the controller shall, without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the Data Protection Officer of this personal data breach unless it is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification does not take place within 72 hours, it shall be accompanied by reasons for the delay.

(2) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

(3) The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) describe the likely consequences of the personal data breach;

(c) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(4) Where, and in so far as, it is not possible to provide details of the breach at the same time, this information may be provided in phases but this shall be done without undue further delay.

(5) The controller shall document any personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Data Protection Officer to verify compliance with this Article.

(6) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without delay. The communication to the data subject shall describe the nature of the personal data breach in clear and plain language.

(7) Details of the complete information to be provided in the notification under paragraph 1 and in the communication under paragraph 6 will be specified in the operational documents.

(8) No communication to the data subject is required if any of the following conditions are met: (i) the controller has implemented appropriate technical and organisational measures, and those measures have been applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (ii) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; (iii) it would involve disproportionate effort, in which case there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(9) If the controller has not already communicated the personal data breach to the data subject, the Data Protection Officer, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 8 are met.

Article 35
Confidentiality of electronic communications

The Office shall ensure the confidentiality of electronic communications, in particular by securing its electronic communications networks.

Article 36
Protection of information transmitted to, stored in, related to, processed by and collected from users' terminal equipment

The Office shall protect the information transmitted to, stored in, related to, processed by and collected from the terminal equipment of users accessing its publicly available websites and mobile applications.

Article 37
Directories of users

(1) Personal data contained in directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.

(2) The Office shall take all the necessary measures to prevent personal data contained in those directories from being used for direct marketing purposes, regardless of whether they are accessible to the public or not.

Article 38
Data protection impact assessment and prior consultation

(1) Where a type of processing, including the setting up or substantial alteration of any files and any automated processing of personal data, is likely to result in a high risk to the rights and freedoms of the data subject by virtue of its context, nature, scope or purpose, the controller shall, prior to the processing, carry out an objective assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) The controller will seek the advice of the Data Protection Officer on the need for a data protection impact assessment and when carrying out any such an assessment. In cases of doubt, the controller will, upon recommendation of the Data Protection Officer, consult the Data Protection Board on the need for a data protection impact assessment and request its opinion.

(3) High risks to the rights and freedoms of data subjects within the meaning of paragraph 1 and the minimum content required in the data protection impact assessment will be defined and further specified in the operational documents.

(4) A data protection impact assessment within the meaning of paragraph 1 is, in particular, required in the case of:

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b. processing on a large scale of special categories of data referred to in Article 11 or of personal data relating to criminal convictions and offences referred to in Article 12; or
c. a systematic monitoring of a publicly accessible area on a large scale.

(5) The Data Protection Board will draw up a list of the kinds of processing operation subject to the requirement of a data protection impact assessment pursuant to paragraph 1. This list will be part of the operational documents. It may also draw up a list of the kinds of processing operation for which no data protection impact assessment is required.

(6) In accordance with Article 39, the controller will consult the Data Protection Board prior to processing where a data protection impact assessment indicates that the processing would result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable security measures as defined in Article 33. The controller will first seek the advice of the Data Protection Officer on the need for prior consultation.

(7) Where the Data Protection Board is of the opinion that the intended processing referred to in paragraph 1 would infringe these Rules, in particular where the controller has insufficiently identified or mitigated the risk, the Data Protection Board will, within a period of up to eight weeks from receipt of the request for consultation, provide the controller and, where applicable, the processor with written advice.

(8) The assessment shall contain at least:

a. a systematic description of the envisaged processing operations and the purposes of the processing;
b. an assessment of the need for and proportionality of the processing operations in relation to the purposes;
c. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with these Rules, taking into account the rights and legitimate interests of data subjects and other persons concerned.

(9) Compliance with approved codes of conduct by the relevant processors shall be duly taken into account in assessing the impact of the processing operations performed by such processors, in particular for the purposes of a data protection impact assessment.

(10) Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of the Office's interests or the security of processing operations.

(11) Where processing pursuant to Article 5(a) or (b) has a legal basis in a legal act adopted on the basis of the European Patent Convention which regulates the specific processing operation or set of operations in question, and where a data protection impact assessment has already been carried out as part of a general impact assessment preceding the adoption of that legal act, paragraphs 1 to 7 will not apply unless that legal act provides otherwise.

(12) Where necessary, the controller will carry out a regular review to assess whether processing is performed in accordance with the data protection impact assessment, at least when there is a change in the risk represented by processing operations in question.

Article 39
Prior consultation of the Data Protection Board

(1) The controller shall consult the Data Protection Board prior to processing where a data protection impact assessment under Article 38 indicates that, in the absence of safeguards, security measures and mechanisms to mitigate the risk, the processing would result in a high risk to the rights and freedoms of natural persons but the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation. The controller shall seek the advice of the Data Protection Officer on the need for prior consultation.

(2) Where the Data Protection Board is of the opinion that the intended processing referred to in paragraph 1 would infringe these Rules, in particular where the controller has insufficiently identified or mitigated the risk, the Data Protection Board shall, within a period of up to eight weeks from receipt of the request for consultation, provide the controller and, where applicable, the processor with written advice and may use any of its powers referred to in Article 47. That period may be extended by six weeks, taking into account the complexity of the intended processing. The Data Protection Board shall inform the controller and, where applicable, the processor of any such extension and the reasons for the delay within one month of receipt of the request for consultation. Those periods may be suspended until the Data Protection Board has obtained information it has requested for the purposes of the consultation.

(3) When consulting the Data Protection Board pursuant to paragraph 1, the controller shall provide it with:

a. where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing;
b. the purposes and means of the intended processing;
c. the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to these Rules;
d. the contact details of the Data Protection Officer;
e. the data protection impact assessment provided for in Article 38; and
f. any other information requested by the Data Protection Board.

VI. Information and consultation

Article 40
Information and consultation of the Data Protection Officer

(1) The controller shall inform the Data Protection Officer when drawing up administrative measures and internal rules relating to the processing of personal data, whether alone or jointly with others.

(2) The controller shall consult the Data Protection Officer when drawing up rules or operational documents related to the implementation of the provisions referred to in Article 25.

VII. Institutional provisions

Article 41
Appointment of the Data Protection Officer

The Data Protection Officer and his or her deputies are appointed by the President of the Office on the basis of their professional qualifications and, in particular, their expert knowledge of data protection law and practices and their ability to fulfil the duties referred to in Articles 43 and 44. The Office will publish their contact details and communicate them to the Data Protection Board.

Article 42
Position of the Data Protection Officer

(1) The Office shall ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The Office shall support the Data Protection Officer in performing the tasks referred to in Article 43 by providing the resources necessary to carry out those tasks, including access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) The Office shall ensure that the Data Protection Officer does not receive any instructions regarding the exercise of those tasks. He or she cannot be dismissed or penalised by the controller or the processor for performing those tasks. The Data Protection Officer reports directly to the President of the Office. Where the proccessing operation is conducted under the organisational autonomy granted to the Boards of Appeal by the President of the Office by virtue of the Act of Delegation, the Data Protection Officer reports directly to the President of the Boards of Appeal.

(4) Data subjects may contact the Data Protection Officer with regard to all issues related to processing of their personal data and to the exercise of their rights under these Rules.

(5) The Data Protection Officer and his or her staff are bound by secrecy or confidentiality as regards the performance of their tasks, both for as long as they perform their functions and after they have ceased to perform them in accordance with the Service Regulations.

(6) The Data Protection Officer may fulfil other tasks and duties. The controller shall ensure that any such tasks and duties do not result in a conflict of interest.

(7) The Data Protection Officer may be consulted, also by informal means, by the controller and the processor and by any individual or any body set up under Article 2 of the Service Regulations on any matter concerning the interpretation or application of these Rules. No one is to suffer prejudice on account of bringing an alleged infringement of these Rules to the attention of the Data Protection Officer.

(8) The Data Protection Officer is appointed for a term of three to five years and eligible for re-appointment. The Data Protection Board shall be consulted prior to any removal of the Data Protection Officer from his or her role where, for example, the position holder no longer fulfils the conditions required for the performance of his or her duties and prior to any termination of his or her appointment as Data Protection Officer on the basis of the relevant provisions of the Service Regulations.

Article 43
Tasks of the Data Protection Officer

(1) The tasks of the Data Protection Officer are:

a. to inform the controller or the processor and the employees who carry out processing of their obligations pursuant to these Rules and to advise them accordingly;
b. to monitor in an independent manner the internal application of and the compliance with these Rules, other legal provisions of the European Patent Organisation having data protection implications and the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities;
c. to raise awareness among and provide training for staff involved in processing operations;
d. to carry out data protection audits and investigations;
e. to ensure that data subjects are informed of their rights and obligations pursuant to these Rules;
f. to provide advice where requested as regards the need to communicate a personal data breach pursuant to Article 34;

g. to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 38, and to consult the Data Protection Board in cases of doubt as to the need for a data protection impact assessment;
h. to provide advice where requested as regards the need for prior consultation of the Data Protection Board pursuant to Article 39;
i. to respond to requests from the Data Protection Board; within the sphere of his or her competence, to co-operate and consult with the Data Protection Board at its request or on his or her own initiative;
j. to facilitate the co-operation between the Data Protection Board and the Office, in particular with regard to data protection investigations, complaint handling, data protection impact assessments and prior consultations, duly informing the Data Protection Board of any recent developments likely to have an impact on the protection of personal data, and forwarding to the Data Protection Board information on new administrative measures and internal rules relating to the processing of personal data;
k. to establish, by way of monitoring, that the rights and freedoms of data subjects are not adversely affected by the Office's processing operations. As a rule, data subjects may at any time consult the Data Protection Officer and submit requests related to processing of their personal data by the Office or the interpretation and implementation of the Rules and it is initially for the Data Protection Officer to respond to such requests. This does not, however, prevent a data subject from using the possibilities of filing a request for review and seeking legal redress under Articles 49 and 50.

(2) The Data Protection Officer may make recommendations to the controller and the processor for the practical improvement of data protection and advise them on matters concerning the application of data protection provisions. Furthermore, he or she may, on his or her own initiative or at the request of the President, the delegated controller, the processor or any body set up under the legal provisions of the European Patent Organisation or of any individual concerned, investigate matters and occurrences directly relating to his or her tasks which come to his or her notice, and report back to the person who commissioned the data protection investigation or to the President of the Office, the delegated controller, the processor or the body set up under the legal provisions of the European Patent Organisation. Where matters and occurrences to be investigated concern the Boards of Appeal Unit, the Data Protection Officer may bring them to the attention of the President of the Boards of Appeal.

(3) The Data Protection Officer shall be informed whenever an issue is under consideration that has, or might have, data protection implications.

(4) If proceedings for the settlement of disputes under Articles 108 to 110a of the Service Regulations involve data protection aspects, the Data Protection Officer shall be consulted in accordance with the procedure provided for in Article 51.

(5) The Data Protection Officer shall have access at all times to the data forming the subject-matter of processing operations and to all offices, data-processing installations and data carriers.

(6) The Data Protection Officer may bring to the attention of the appointing authority any failure by an employee to comply with the obligations under these Rules and, where appropriate, recommend that an administrative investigation be launched to establish whether any action needs to be taken in accordance with the Service Regulations. Where the employee in question is allocated to the Boards of Appeal Unit, the Data Protection Officer may also bring such a failure to comply with the obligations under these Rules to the attention of the President of the Boards of Appeal.

(7) The Data Protection Officer will submit an annual report to the Administrative Council, the President of the Office, and the President of the Boards of Appeal.

Article 44
Deputy Data Protection Officers

(1) The Deputy Data Protection Officers will support the Data Protection Officer in carrying out his or her tasks and duties and deputise in the event of his or her absence. The Deputy Data Protection Officers and any staff assisting the Data Protection Officer in relation to data protection issues will act solely on his or her instructions. The Deputy Data Protection Officers will be chosen in such a way as to ensure an adequate representation of the fields of expertise required in data protection matters.

(2) Article 42 (2), (5) and (8) applies *mutatis mutandis* to the Deputy Data Protection Officers.

(3) The Data Protection Officer may ask the Deputy Data Protection Officers to perform certain tasks independently.

Article 45
Data Protection Liaisons

(1) At least one Data Protection Liaison is to be appointed in each operational unit unless the delegated controller decides otherwise for operational reasons.

(2) The Data Protection Liaison's function can be combined with other functions as appropriate. To acquire the skills required to perform their function, Data Protection Liaisons will undergo compulsory training on data protection.

(3) Data Protection Liaisons will be appointed for a renewable term of one to three years. They will be chosen, at the appropriate hierarchical level, on the basis of their high professional ethics, their knowledge and experience of the workings of their operational unit and their motivation to perform the function.

(4) Without prejudice to the responsibilities of the Data Protection Officer or the controller, the Data Protection Liaisons will assist the controller in complying with its legal obligations.

Article 46
Obligation to provide assistance and information

Every employee and all operational units of the Office and bodies within the meaning of Article 2 of the Service Regulations are required to assist the Data Protection Officer, his or her Deputies and the Data Protection Liaisons in performing their duties. To enable the Data Protection Officer and, where appropriate, the Deputy Data Protection Officers to assess compliance with these Rules, they shall, at the Data Protection Officer's request, be:

a. given information in reply to questions and be allowed to inspect all documents and all data stored in files and any data processing programmes;
b. allowed access to all information, including personal data as well as processing operations, required to perform their tasks; and
c. given access at all times to all EPO offices, data-processing installations and data carriers.

Article 47
Data Protection Board

(1) The Data Protection Board has an oversight and advisory function and a function as part of the mechanism for legal redress under Article 50. It is responsible for:

a. monitoring, together with the Data Protection Officer, the application of these Rules and the operational documents to all data processing operations carried out by the Office;
b. requesting, where appropriate, co-operation from the delegated controllers and the controller in the performance of its tasks;
c. providing consultation for the President of the Office in cases of doubt on the adequacy of the protection afforded by a country or international organisation under Article 9(3);
d. overseeing the processing of data relating to criminal offences, criminal convictions or security measures under Article 5 where such processing is not covered by the legal provisions of the European Patent Organisation as provided in Article 12.

(2) Pursuant to Articles 38 and 39, the Data Protection Board:

a. issues an opinion on the need for a data protection impact assessment following a request from the controller;
b. draws up a list of the kinds of processing operation for which a data protection impact assessment is required and may draw up a list of the kinds of processing operation for which no data protection impact assessment is required;
c. provides consultation for the controller, upon a recommendation from the Data Protection Officer, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable security measures as defined in Article 38(6).
d. provides written advice to the controller, and where applicable to the processor, where it is of the opinion that the intended processing referred to Article 38(6) would infringe these Rules, in particular where the controller has insufficiently identified or mitigated the risk.

(3) The Data Protection Board is responsible for:

a. advising under Article 42(8) on dismissal of the Data Protection Officer if he or she no longer fulfils the conditions required for the performance of his or her duties;
b. providing an opinion where a data subject makes use of the means of redress available under Article 50.

Article 48
Appointment and composition of the Data Protection Board

(1) The Data Protection Board is composed of three external experts in the field of data protection appointed by the President of the Office, namely a chair and two other members, one of whom acts as deputy chair. Two alternate members are to be appointed to replace these two other members if they are unable to act. The Chair may invite the Data Protection Officer or, exceptionally, other parties to the meetings of the Data Protection Board as observers.

(2) The chair, the two other members and the alternate members shall have the qualifications required for appointment to 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 shall not be Office employees in active service or have been employed by it within the past ten years.

(3) The chair, the other two members and the alternate members of the Data Protection Board enjoy the privileges and immunities conferred under Article 15 of the Protocol on Privileges and Immunities of the European Patent Organisation when exercising their duties as members of the Data Protection Board.

(4) The chair, the other two members and the alternate members are appointed for a renewable term of three years.

(5) The chair, the other two members and the alternate members of the Data Protection Board are bound by an obligation of confidentiality which continues indefinitely after their term comes to an end.

(6) The chair, the other two members and the alternate members of the Data Protection Board are completely independent in carrying out their functions. They shall not seek nor be bound by instructions from the Office or the Administrative Council.

(7) The chair, the other two members and the alternate members of the Data Protection Board shall refrain from acting in a case in which they have a conflict of interest, in particular a personal interest.

(8) Where the chair of the Data Protection Board is prevented from acting, he or she will be replaced by the deputy chair. A member of the Data Protection Board who is prevented from acting will be replaced by an alternate member nominated by the chair.

(9) In proceedings under Article 50, the Data Protection Board will be bound by separate rules of procedure adopted by the President after consultation of the President of the Boards of Appeal and submitted for information to the Administrative Council.

(10) The Office shall support the Data Protection Board in performing the tasks referred to in this Article by providing the resources necessary to carry out those tasks, the legal and administrative support of a Secretariat and access to personal data and processing operations.

Article 49
Request for review by the delegated controller

(1) Data subjects who consider that the processing by the Office of their personal data infringes their rights as a data subject under these Rules may request that the delegated controller review the matter and take a decision. The request shall 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.

(2) Prior to taking any decision, the delegated controller shall consult the Data Protection Officer. The Data Protection Officer shall provide the delegated controller with a written opinion no later than 15 calendar days after receipt of the request for review. If the Data Protection Officer has not provided an opinion by the end of this period, it will no longer be required.

(3) The decision under paragraph 1 above shall be taken within one month of receipt of the request, and communicated to the data subject in writing, indicating the means of redress provided for in Article 50. This time limit may be extended by two further months where necessary, taking into account the complexity and number of the requests. If it is necessary to extend the standard time limit, the delegated controller shall duly notify the data subject of this and the reasons for the delay within one month of receipt of the request for review. If the controller or the delegated controller fails to take any action by the end of a period of three months, this will be deemed to be an implicit rejection of the request.

(4) A decision or implicit rejection by the delegated controller under this Article is a condition for filing a complaint with the Data Protection Board under Article 50.

Article 50
Legal redress

(1) Data subjects may challenge the decision taken under Article 49(1) by filing a complaint with the Data Protection Board within three months of receipt of the decision in accordance with Article 49(3) or, in the case of an implicit rejection, of the date of expiry of the time limit for replying to the request for review.

(2) When examining an objection filed by a data subject, the Data Protection Board shall invite the data subject, the delegated 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 evidence already at hand.

(3) After examining the objection, the evidence and any written input submitted by the data subject, the delegated controller and, where applicable, the processor, the Data Protection Board shall issue a reasoned opinion to the controller. If it finds that the Office's processing of the data subject's personal data was unlawful, it may recommend that compensation for material and/or non-material damage be awarded.

(4) The Data Protection Board shall communicate its reasoned opinion to the controller, which will then take a final decision. The controller will normally follow the Data Protection Board's opinion. If the controller decides not to follow the opinion, it shall set out in writing the reasons for deviating from it.

(5) When the President of the Boards of Appeal acts as the controller under the organisational autonomy granted by the Act of Delegation, he or she shall inform the President of the Office of his or her final decision. When the President of the Office takes a final decision on a complaint lodged with the Data Protection Board and concerning activities of the Boards of Appeal in which the President of the Boards of Appeal acts as the delegated controller, he or she shall inform the President of the Boards of Appeal.

(6) The controller shall notify the data subject, the delegated controller and, where applicable, the processor, as well as the Data Protection Officer, of the final decision and the conclusions of the Data Protection Board. A copy of the decision shall also be sent to the Data Protection Board.

(7) The persons covered by Article 1 of the Service Regulations may challenge the decision of the controller only before the Administrative Tribunal of the International Labour Organization under Article 113 of the Service Regulations.

(8) If data subjects not covered by Article 1 of the Service Regulations disagree with the decision taken by the controller, they may ask the President of the Office, within three months of receipt of the final decision under paragraph 6, for ad-hoc arbitration proceedings under Article 52 to resolve their dispute with the Office over the processing of their personal data.

(9) In cases in which the final decision challenged under paragraphs 7 and 8 of this Article was taken by the President of the Boards of Appeal, he or she shall be informed that the decision has been challenged.

Article 51
Incidental data protection request during internal appeal proceedings

(1) Where proceedings for the settlement of disputes under Articles 108 to 110a of the Service Regulations involve data protection aspects, the Data Protection Officer shall be consulted by the body under the Service Regulations advising the appointing authority before delivering its opinion or, at the latest, by the competent appointing authority before taking its decision.

(2) The Data Protection Officer shall deliver his or her opinion in writing no later than 15 calendar days after receipt of the request for consultation under paragraph 1. If the Data Protection Officer has not provided his or her opinion by the end of this period, it is no longer required.

(3) Where the Data Protection Officer's opinion has been requested during proceedings for the settlement of disputes under Articles 108 to 110a of the Service Regulations, the proceedings may be suspended for the time needed to provide that opinion but in any event for no longer than 15 calendar days.

(4) The appointing authority is not bound by the Data Protection Officer's opinion.

Article 52
Ad-hoc arbitration

(1) Any dispute, controversy or claim raised by a data subject not falling within the scope of application of Article 1 of the Service Regulations arising from a decision of the controller notified to the data subject in accordance with Article 50(6) shall be the subject of final and binding arbitration in accordance with the following procedure and to the exclusion of any other national or international jurisdiction.

(2) Within three months of receipt of the controller's final decision under Article 50(6), the data subject may request the President of the Office in writing to initiate the arbitration procedure set forth in these Rules.

(3) Within three months of receipt of such notification by the data subject, one arbitrator shall be appointed by the Secretary-General of the Permanent Court of Arbitration.

(4) The arbitrator shall be legally qualified, admitted to practise law in one of the contracting states and be able to demonstrate relevant expertise in data protection matters. He or she shall be familiar with the law governing international organisations. The arbitrator must not be or have been in or at the service of the Office or the data subject. He or she shall act independently and impartially.

(5) The place of arbitration shall be The Hague (the Netherlands).

(6) The law governing the arbitration procedure shall be the European Patent Convention, these Rules, including any implementing legislation, the law of international organisations and the principles of public international law.

(7) The language of the proceedings shall be one of the official languages of the Office (English, French or German), as determined by the arbitrator.

(8) Subject to this Article, the arbitrator may conduct the arbitration as he or she sees fit, provided that the parties are treated equally and each party is given the opportunity of presenting his or her case at every stage of the proceedings.

(9) The arbitration proceedings are not public. The parties and the arbitrator shall treat the subject-matter of the proceedings confidentially. The arbitration award shall not be published.

(10) A settlement shall be concluded in the form of a written arbitration award with an agreed wording.

(11) The arbitrator shall fix the costs of arbitration in his or her award. The term "costs" includes the fees of the arbitrator, travel and other reasonable expenses incurred by the arbitrator, reasonable costs of expert advice required by the arbitrator and reasonable travel and other expenses of witnesses. The fees of the arbitrator shall be reasonable in amount, taking into account the complexity of the subject-matter, the time spent, the value of the dispute (if any) and other relevant circumstances of the case. Promptly after his or her appointment, the arbitrator shall inform the parties as to how he or she proposes to determine his or her fees and expenses. Within 15 calendar days of receiving that proposal, any party may refer the proposal to the Secretary-General of the Permanent Court of Arbitration for review. If the Secretary-General of the Permanent Court of Arbitration finds that the proposal is inconsistent with the principles of this paragraph, he or she shall make any necessary adjustments, which shall be binding upon the arbitrator.

(12) The arbitrator fixes the value of the dispute by exercising his or her reasonable discretion.

(13) The European Patent Organisation pays the arbitrator's fees and expenses, the cost of possible expert advice and witnesses. Each party pays his or her own costs for legal representation and expenses unless the arbitrator decides otherwise.

VIII. Final provisions

Article 53
Right to compensation

(1) Any person who proves that he or she has suffered damage as a result of an infringement of these Rules may request compensation from the Office using the means of redress offered under Articles 49 and 50.

(2) The controller or processor shall be exempt from liability under paragraph 1 if it proves that it was not responsible for the event giving rise to the damage.

Article 54
Sanctions

Any employee failing to comply with the obligations laid down in these Rules, whether intentionally or through negligence, may be liable to disciplinary or other action in accordance with the Service Regulations.

Article 55
Transitional provisions

(1) The data collected up to the entry into force of these Rules will be deemed to have been lawfully collected within the meaning of Article 4.

(2) Processing operations initiated after the adoption of these Rules shall comply with the requirements laid down in these Rules.

(3) Processing operations which are already ongoing on the date of the adoption of these Rules shall be brought into line with the requirements laid down in these Rules within six months of the entry into force of these Rules. In exceptional cases, for which due justification shall be presented, the Data Protection Officer may allow this time limit to be extended.

(4) The records for processing operations already entered in the Data Protection Register or covered by existing documents on the use of personal data shall be revised by the operational units concerned, brought into line with the new requirements and entered in the new central register within six months of the entry into force of these Rules.

(5) As to restriction of rights under Article 25: specific provisions will be adopted by the President of the Office, in consultation with the Data Protection Officer and the President of the Boards of Appeal, before entry into force of these Rules.

Article 56
Entry into force/Revision

(1) These Rules enter into force on 1 January 2022 and apply to any processing of personal data ongoing on or initiated after that date.

(2) These Rules should be reviewed no later than five years after they have entered into force.