

# **GUIDELINES FOR THE PROTECTION OF PERSONAL DATA IN THE EUROPEAN PATENT OFFICE<sup>1</sup>**

<sup>1</sup> References in these guidelines to the Data Protection Officer and other persons are to be regarded as applying to persons of either sex.

## **Preamble**

The purpose of these guidelines is to ensure that every person whose personal data are used by the European Patent Office (EPO) is guaranteed protection of his privacy with regard to the handling of his personal data. It shall also provide guidance for all EPO staff on the permissible use and handling of personal data, including and with specific reference to, operational data, acknowledging the need for the smooth operation of services and administration of employment relationships.

## **I. General provisions**

### **Article 1**

#### **Purpose of the guidelines**

- (1) The European Patent Office shall protect the rights of natural persons to privacy with respect to the processing of personal data.
- (2) The Data Protection Officer appointed under Article 18 of these guidelines shall monitor the observance of these guidelines with respect to all processing operations performed by the European Patent Office. He shall be independent in his function.

### **Article 2**

#### **Definitions**

For the purposes of these guidelines:

- a) "personal data" means any information relating to any identified or identifiable natural person (hereinafter referred to as "data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, economic, cultural or social identity; an individual is not considered "identifiable" if identification requires unreasonable time or effort;
- b) "operational data" is personal data considered to belong to the data essential for the management and/or administration of the activities and tasks of the European Patent Office. For the purpose of these guidelines, operational data are expressed in the form of data sets. Explicit definitions of these data sets and of the persons authorised to use them are to be given in a Document on the Use of Operational Data relating to that operational unit.
- c) "Document on the Use of Operational Data "DUOD" means an additional document which is to be drawn up by the controller of operational data in agreement with the Data Protection Officer. It should specify more detailed requirements and procedures relating to the governance and management of operational data and comprises descriptions of required behaviour, responsibilities and actions expected of employees with regard to the management, use and processing of data. Further, it comprises a list of operational data, authorised user groups for operational data, permissible purposes for the use of data, and any further regulations which are relevant to data processing within that operational unit.
- d) "file" means any structured set of personal data which are accessible and can be evaluated according to personal criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- e) "processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or

otherwise making available, alignment or combination, blocking, erasure or destruction;

- f) "storage" means the capture, inclusion or archiving of personal data on a data carrier;
- g) "amendment" means altering the content of stored data;
- h) "transmission" means the communication of personal data to recipients other than the data subject or within the domain of the controller, whether or not the data are passed on immediately or retained for consultation or retrieval or made accessible in some other form;
- i) "erasure of data" means the obliteration of stored data in such a way that reconstruction is not possible (physical erasure) as well as the permanent prevention of access to data by programming measures (logical erasure);
- j) "controller" means the natural person who determines the purposes and means of the processing of personal data or to whom the President has assigned the responsibility for processing personal data;
- k) "processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
- 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 the data;
- m) "recipient" means a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not;
- n) "the data subject's consent" means any specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;
- o) "employee" means every person mentioned in Article 1 of the Service Regulations and all contract staff;
- p) "operational unit" means an organisational unit or - independent of the organisational structure - a project or group of people working to perform a task and/or activities within the EPO;
- q) "monitoring an individual's conduct" means any checking by the Office of data related to an employee's conduct for a specific purpose;
- r) "monitoring an individual's performance" means any checking by the Office of the work performed by any identified or identifiable employee including inter alia ability, efficiency, quantity, or quality. Monitoring an individual's performance also means the checking of certain aspects of the work performed or the checking of specific steps in procedures carried out by him or under his supervision.
- s) "internal investigative processes" mean the codified internal investigative processes such as the investigative process according to the Guidelines for Investigations at the EPO (Circular No. 342) or the Policy on the prevention of harassment and resolution of conflicts at the EPO (Circular No. 341) or the Guidelines on the use of electronic communication systems (Communiqué No. 10).

### **Article 3**

#### **Scope of the guidelines**

These guidelines apply to the processing of personal data by the European Patent Office. They apply to the processing of personal data wholly or partly by automatic means, and to the processing other than by automatic means of personal data wherever such data form part of a file or are intended to form part of a file.

## **II. General rules on the lawfulness of the processing of personal data**

### **Article 4**

#### **Principles relating to data quality**

- (1) Personal data shall be
  - a) processed fairly and lawfully;
  - b) collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with these purposes. Further processing of personal data for statistical purposes is not considered incompatible with the original purpose provided that there are safeguards in place to ensure the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual;
  - c) adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed;
  - d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that 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;
  - e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed; personal data which are to be stored for longer periods for historical, statistical or scientific use shall be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, these data shall not be used for anything other than for historical, statistical or scientific purposes.
- (2) Personal data shall as a general rule and wherever possible be collected from the data subject.
- (3) When processing personal data and in particular when designing and selecting computer systems, the European Patent Office shall aim to process as little personal data as possible. In particular, anonymity and pseudonymity shall be applied wherever possible and wherever the effort involved is in proportion to said principle.
- (4) The controller shall ensure that the principles set out in this article are observed.

### **Article 5**

#### **Lawfulness of processing personal data**

Personal data may be processed only if

- a) processing is necessary for the performance of a task carried out on the basis of the European Patent Convention or other legal instruments adopted on the basis thereof or in the legitimate exercise of the official authority vested in the European Patent Office or in a third party to whom the data are transmitted; this shall also include the management of the Information Systems; or
- b) processing is necessary for administering, terminating or winding up a relationship of service or former service, or
- c) processing is necessary for compliance with a legal obligation to which the controller or the controller's entity is subject, or
- d) 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
- e) the data subject has given his consent, or
- f) processing is necessary in order to protect the vital interests of the data subject, or

- g) there is no possibility of obtaining the data subject's consent or to do so would involve going to disproportionate lengths, but it is obvious under the circumstances that such processing is in his interest.

## **Article 6**

### **Change of purpose**

- (1) Without prejudice to Articles 4, 5, 9 and 11, personal data may only be processed for purposes other than those for which they have been collected if the change of purpose is approved by the President following consultation of the Data Protection Officer.
- (2) Without prejudice to Articles 4, 5 and 11, personal data collected for the sole purpose of monitoring or ensuring the security of processing systems or operations may not be used for any purpose other than the investigation, ascertainment and prosecution of serious offences. **This restriction shall not apply to internal investigative processes.**
- (3) Processing operations carried out by the Information Services of the European Patent Office with the sole purpose of ensuring continuous operations and root cause analysis of malfunctions shall not be considered as falling under this Article.

## **Article 7**

### **Transmission of personal data to recipients within the European Patent Organisation**

Without prejudice to Articles 4, 5, 6, 9 and 11:

- (1) Personal data may only be transmitted within the European Patent Organisation if the data are necessary for the performance of tasks covered by the competence of the recipient.
- (2) Where the data are transmitted following a request from the recipient, both the controller and the recipient bear the responsibility for the legitimacy of such transmission.
- (3) The recipient may process the personal data only for the purposes for which they were transmitted.

## **Article 8**

### **Transmission to recipients outside the European Patent Organisation**

- (1) The transmission of personal data to recipients outside the European Patent Organisation is only permissible if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transmitted solely to allow tasks covered by the competence of the controller to be carried out.
- (2) The adequacy of the level of protection afforded by the country or international organisation in question must be assessed in the light of all the circumstances surrounding a data transmission operation or set of data transmission operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient country or recipient international organisation, the rules of law in force in the country or international organisation in question and the professional rules and security measures which apply in that country or international organisation.
- (3) An adequate level of protection is regarded as being ensured in countries whose national legislation meets the requirements of Directive 95/46/EC of the European Parliament and the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and any amendments thereto.
- (4) In cases of doubt, the President decides on the adequacy of the protection afforded by the relevant country or international organisation.**
- (5) The transmission of personal data to recipients outside the European Patent Organisation is also permissible where

- a) the data subject has given his consent;
  - b) the data are requested in connection with legal proceedings and their transmission is not precluded by agreements under international law or regulations laid down by the Administrative Council;
  - c) the transmission takes place on the basis of the European Patent Convention and its constituent parts, international agreements concluded by the President under his general mandate or under a special mandate from the Administrative Council, or regulations laid down by the Administrative Council;
  - d) the transmission is necessary in order to protect the vital interests of the data subject;
  - e) the transmission is necessary to avert serious threats to public security while having due regard to the principle of proportionality;
  - f) the transmission is made from a register which according to the law 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 consultation are fulfilled in the particular case.
- (6) Without prejudice to paragraph 5, the President may authorise a transfer or a set of transfers of personal data to a third country or international organisation which does not ensure an adequate level of protection within the meaning of this Article, where the controller adduces adequate safeguards with respect to the protection of the privacy of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.
- (7) The data transmitted under this article may only be processed or used for the purpose for which they have been transmitted. They must be deleted as soon as that purpose has been achieved. The recipient must be advised and obliged accordingly.

### **III. Special provisions relating to processing**

#### **Article 9**

#### **Processing special categories of data**

- (1) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and of data concerning health or sex life, is prohibited.
- (2) Paragraph 1 shall not apply where
  - a) the data subject has given his consent to the processing of those data,
  - b) processing is necessary to comply with the legal obligations of the European Patent Office in the field of employment law insofar as this is authorised by the European Patent Convention or other legal instruments adopted on the basis thereof,
  - 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 his consent, or
  - d) processing relates to data which have been made public by the data subject.
- (3) Nor shall paragraph 1 apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of health care or treatment, the management of health-care services or for medical examinations and opinions provided for in the Service Regulations or Circulars and Communiqués and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

(4)

a) Processing of data relating to offences, criminal convictions or security measures may be carried out only if the European Patent Organisation's interest therein is legitimate and outweighs other interests and the case in question has been approved by the President following consultation of the Data Protection Officer.

b) This requirement shall not apply to internal investigative processes.

#### **Article 10**

##### **Processing of operational data**

Operational data (as defined in the Document on the Use of Operational Data) may be processed by authorised users (also defined in the Document on the Use of Operational Data) for all general management and administrative purposes, provided that any use of data relating to individuals is strictly limited to the operational unit for which that Document on the Use of Operational Data applies. Further restrictions as defined in the Document on the Use of Operational Data must be observed. Combinations with non-operational data, as well as alterations of the purpose of the processing, shall not be covered by this exemption. Article 11 of these guidelines shall not be affected by this provision.

#### **Article 11**

##### **Processing operations which are subject to approval**

- (1) The setting up or substantial alteration of any files and any automated processing of personal data likely to present specific risks to the privacy rights of the data subject by virtue of their content, nature, scope or purpose is subject to approval by the President.
- (2) Specific risks for the privacy rights of data subjects within the meaning of paragraph 1 are posed in particular by
  - a) the processing of particular data categories in accordance with Article 9, paragraph 1,
  - b) a processing operation that enables unforeseen alignment of data which can be processed or have been processed for different purposes,
  - c) a processing operation for the purpose of excluding individuals from a right, benefit or contract,
  - d) the transmission of data to recipients outside the European Patent Organisation.
- (3) The Data Protection Officer shall be notified prior to the setting up or substantial alteration of any file or automated processing operation which is likely to come under the scope of paragraphs 1 and 2. If the Data Protection Officer is of the view that the file or automated processing operation presents specific risks for the data subject's privacy rights in view of the content, nature, scope or purpose thereof, he shall submit such notification, along with a reasoned opinion, within 15 working days to the President for approval and shall advise the notifying department accordingly.
- (4) This article shall not apply to processing operations involving exclusively the use of operational data and complying with the Document on the Use of Operational Data in force at the time.

#### **Article 12**

##### **Use of data to monitor an individual's conduct and performance by the Office**

- (1) Personal data electronically collected for other purposes may only be used to monitor an individual's conduct when the particular case has been approved by the President following consultation of the Data Protection Officer and the data subject has been informed accordingly.

This provision does not apply

- a) to the mere retrieval of personal data involving no further processing by persons with authorised access, provided this is for the purposes for which the data were collected, and

b) to internal investigative processes.

- (2) Personal data may only be used to monitor an individual's performance if it has been defined as operational data and if the DUOD in force at the time permits such use and sets out the use and scope, access of the employee to this data, and time limits for the use of data for this purpose.

#### IV. Information to be supplied to data subjects and rights of data subjects

##### Article 13

##### Information to be supplied

- (1) Where personal data are stored or transmitted, the controller shall provide the data subject promptly with at least the following information:
- a) the identity of the controller,
  - b) the purposes of the processing operation for which the data are intended,
  - c) the data categories processed,
  - d) the data recipients or categories of data recipients, where applicable,
  - e) the entitlement to information and to have wrong or inaccurate data corrected wherever those data relate to him.

(2) No duty to inform under paragraph 1 exists where

- a) the data subject has learned by other means of the information listed in paragraph 1 or could have been expected to learn of it, in particular when the processing operation is entered in the data protection register maintained under Article 23,
- b) it is impossible to inform the data subject or this requires undue effort, or
- c) storing or transmitting personal data is expressly provided for in the European Patent Convention or its constituent parts, in international agreements concluded by the President under his general mandate or under a special mandate from the Administrative Council, or in regulations laid down by the Administrative Council.

d) the information under these Guidelines would conflict with the information duties as foreseen in regulations on internal investigative processes.

- (3) If the processing operation concerns over 100 data subjects, they may be informed by way of generally accessible data protection statements that form part of the data protection register.

##### Article 14

##### Rights of the data subject

- (1) Unless the data subject has direct access to the data in question, he is entitled to obtain from the controller, freely and without hindrance, the following information, free of charge, at any time and at intervals that are reasonable and correspond to the nature of the data, within three months of making a request to that effect:
- a) confirmation as to whether data relating to him are being processed,
  - b) details of the purposes of any such processing, the legal basis therefore, the data categories being processed, the recipients or categories of recipients to whom the data are being transmitted, and the timeframe to which the data in question relate,
  - c) notification in an intelligible form of the data undergoing processing and of all available information as

to their source,

d) information about the logical structure of any automated processing of data concerning him.

- (2) At the data subject's request, the controller shall rectify without delay incorrect or incomplete personal data.
- (3) At the data subject's request, the controller shall block data if
  - a) the data subject challenges their accuracy on compelling legitimate grounds, for a period allowing the controller to check the accuracy, including the completeness, of the data, or
  - b) the controller no longer needs them to perform his duties, but they must be retained for evidentiary purposes, or
  - c) the processing is unlawful, but the data subject objects to their deletion and instead demands that they be blocked instead.
- (4) Automated files are generally blocked by technical means. The blocking of personal data is to be indicated in the system in such a way that it is clear that the personal data may not be used. Blocked personal data may only be processed, apart from being stored, if they are required for evidentiary purposes, if the data subject has given his consent or if the data are necessary to protect the rights of third parties. A data subject who has requested the blocking of such data and has had them blocked shall be informed by the controller prior to their being unblocked.
- (5) At the data subject's request, the controller shall delete data if their processing is unlawful, in particular in the event of infringement of the provisions of Articles 4 to 12.
- (6) At the data subject's request, the controller shall notify the third parties to whom the data have been transmitted of any correction, deletion or blocking of data made in accordance with this article, unless this proves to be impossible or requires undue effort.
- (7) If requests under paragraph 1 cannot be fulfilled within three months, the Data Protection Officer can extend this time limit at the controller's request. Any such extension shall be notified to the requester.
- (8) Where the provisions of this Article conflict with the provisions for internal investigative processes, the provisions on internal investigative processes shall prevail.

#### **Article 15**

##### **The right of the data subject to object**

The data subject has the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, except in the cases covered by Article 5 (a), (b), (c) and (d). Where the President finds that the objection is justified, the processing in question may no longer involve those data.

#### **V. Confidentiality and security of processing**

##### **Article 16**

##### **Confidentiality and security of processing**

- (1) Personal data may only be processed by the controller or on his instructions, unless stated otherwise in the legal provisions of the European Patent Organisation.
- (2) The European Patent Office shall take the technical and organisational measures required to secure data against accidental destruction or loss and against unauthorised access, alteration or dissemination. In particular, the circle of persons with authorised access must be fixed by the controller of the file in question and kept to a strict minimum. Specific requirements as to data security are annexed to these

guidelines as Annex 1.

#### **Article 17**

##### **Processing of personal data on behalf of the controller**

- (1) The controller may only assign the task of processing personal data to a processor if the latter provides sufficient warranties of compliance with the technical and organisational security measures under Article 16, paragraph 2. The controller remains responsible for compliance with those measures.
- (2) Personal data may be processed on behalf of the controller only if a contract or legal instrument exists obliging the processor in particular to
  - a) ensure compliance with the principles set out in Article 16, paragraph 2,
  - b) act exclusively on the controller's instructions, and
  - c) ensure compliance with the principles set out in Article 4.
- (3) This commitment shall be documented in writing and shall include in particular
  - a) subject and duration of the work to be carried out,
  - b) the extent, type and purpose of the intended data processing,
  - c) the rectification, erasure and blocking of data,
  - d) any right to issue subcontracts,
  - e) the controller's rights to monitor and the processor's corresponding obligations to accept and cooperate,
  - f) the duty of the processor to employ only staff who have committed themselves to confidentiality,
  - g) the duty of the processor to notify the controller of any breach of data protection provisions, and
  - h) the return of data storage media and/or the erasure of data recorded by the processor after the work has been carried out.
- (4) The Data Protection Officer shall be informed of every processing operation on behalf of the controller, accompanied by evidence as specified in paragraphs 1 to 3.

#### **VI. Institutional provisions**

##### **Article 18**

##### **Data Protection Officer**

- (1) The Data Protection Officer and his deputy shall be appointed by the President.
- (2) The term of office of the Data Protection Officer shall be two years; he may be reappointed.
- (3) The Data Protection Officer shall not be required to follow instructions when carrying out his duties in connection with data protection; the fact of performing such duties may in no way be prejudicial to him.
- (4) The Data Protection Officer shall be provided with the staff and financial and other resources required for the performance of his duties. To the extent required, he, his deputy and any other staff assigned to him shall be released from other activities.
- (5) The Data Protection Officer, his deputy and his staff shall be bound to confidentiality both during the exercise of their functions and after they have ceased to perform them.

## **Article 19**

### **Duties of the Data Protection Officer**

- (1) As laid down in Article 1, paragraph 2 of these guidelines, the Data Protection Officer shall monitor the observance of these guidelines with respect to all processing operations performed by the European Patent Office. For this purpose he may make recommendations for the practical improvement of data protection and advise the President and organisational units of the European Patent Office on questions concerning the application of data protection.
- (2) The Data Protection Officer shall of his own accord or at the request of the President, an Office department, a body under the Service Regulations or a data subject examine any matters and occurrences directly relating to his field of duties that come to his notice. The Data Protection Officer shall inform the concerned department of the findings.
- (3) The Data Protection Officer may request the President to order the rectification, blocking, or erasure of all data processed in breach of these guidelines and the notification of such an order to third parties to whom the data have been disclosed. He may also request the President to impose a temporary or definitive ban on such processing.
- (4) The Data Protection Officer shall, where appropriate, make recommendations to the President for changes to these guidelines.
- (5) The Data Protection Officer shall provide expert advice and opinions on request and draw up reports.
- (6) The Data Protection Officer shall submit an activities report to the President each year.
- (7) The Data Protection Officer shall also have the duties assigned to him in these guidelines.

## **Article 20**

### **Data Protection Deputy**

- (1) A Data Protection Deputy shall assist the Data Protection Officer in performing his tasks. He shall be appointed by the President. The Deputy shall be accountable to the Data Protection Officer, but otherwise shall not be required to follow instructions in his capacity as Data Protection Deputy; the fact of performing such duties may in no way be prejudicial to him. The Data Protection Deputy shall be chosen to ensure an adequate representation of the fields of expertise required in data protection matters.
- (2) Article 18, paragraphs 2, 4 and 5, applies *mutatis mutandis* to the Data Protection Deputy.
- (3) The Data Protection Officer may ask the Data Protection Deputy to perform certain tasks independently.

## **Article 21**

### **Obligation to provide information and assistance**

Every employee and all departments and bodies of the European Patent Office shall be required to assist the Data Protection Officer and his Deputy in performing their duties. To enable the Data Protection Officer, and where appropriate the Data Protection Deputy, to assess compliance with these Guidelines, they

- a) shall be given information in reply to questions and be allowed to inspect all documents and in particular all data stored in files and any data processing programs,
- b) shall be allowed access to all information required for their evaluations,
- c) shall be allowed access at all times to all offices and to all data processing installations and data carriers; the DPO shall ask a neutral third person who is not connected to the matter to be physically present when access is given.

## **Article 22**

### **Duties of the controller**

The controller is responsible in particular for monitoring observance of the restrictions on the purpose-related use of data and the extent of such use. Where applicable, he shall advise users of the data of the possible consequences of infringement. Should he become aware of a major or repeated infringement, he shall inform the President or the Data Protection Officer accordingly. Other special provisions, such as in particular Articles 18, 19 of these Guidelines, shall not apply to him.

## **Article 23**

### **Data protection register**

- (1) Any processing of personal data that is subject to approval under Article 11 shall be entered in the data protection register. The following information shall be entered in respect of each processing operation:
  - a) the controller,
  - b) the purposes of the processing operation,
  - c) the data-subject categories,
  - d) a description of the data or data categories,
  - e) the recipient(s) or recipient categories,
  - f) the time limits by which the data or data categories will be blocked or deleted,
  - g) whether personal data are to be transmitted to bodies outside the European Patent Office,
  - h) the names of the persons having access to the data processing programs and restrictions where applicable,
  - i) the measures taken under Article 16, paragraph 2, to ensure that personal data are processed securely.
- (2) The data protection register is kept by the Data Protection Officer. It may be inspected by any data subject.

## **Article 24**

### **Complaints**

- (1) If the Data Protection Officer finds that these guidelines or annexes thereto have been infringed or that there are other deficiencies in the processing of personal data, he shall invite the controller to comment within a reasonable time limit. The Data Protection Officer may make proposals for eliminating the deficiencies noted in his invitation to comment. Such comment shall also set out the measures that are proposed or have already been taken to remedy the deficiencies noted by the Data Protection Officer.
- (2) In the case of minor deficiencies or deficiencies that have already been eliminated, the Data Protection Officer may decide not to lodge a complaint or not to ask the relevant department to comment.
- (3) In the case of major infringements of these guidelines or failure to eliminate the deficiencies noted, the Data Protection Officer shall notify the President.

## **Article 25**

### **Application to the Data Protection Officer**

- (1) Any data subject may apply to the Data Protection Officer for advice on data protection matters or if the data subject thinks that his rights have been infringed in the course of processing his personal data or that there has been any other infringement under these guidelines.

- (2) Prior to taking any decisions relating to individuals within the meaning of Article 106 of the Service Regulations that concern data protection, the President shall obtain a written opinion on the issue in question from the Data Protection Officer. The Data Protection Officer shall deliver his opinion without delay. After 15 working days an opinion shall no longer be necessary.
- (3) If an internal appeal is lodged on a matter relating to data protection, the Data Protection Officer may submit his opinion either on his own initiative to the President, or at the request of the appellant or the Chair of the Internal Appeals Committee to the Internal Appeals Committee.

## **VII. Final provisions**

### **Article 26 Sanctions**

Any employee in breach of his obligations under these guidelines shall be liable under Article 93 of the Service Regulations and, where the circumstances demand, also for damages under the relevant regulations.

### **Article 27 Transitional provisions**

- (1) The data collected up to the entry into force of these guidelines shall be deemed to have been lawfully collected within the meaning of Article 4.
- (2)
  - a) Processing operations which are already under way on the date of entry into force of these guidelines shall be brought into line with these guidelines within six months of that date.
  - b) If the processing operations have already been entered in the data protection register under Article 17 of the Guidelines for the Protection of Personal Data in the European Patent Office (version in force since 29 June 1992), they do not have to be declared again in accordance with Article 11 of these guidelines. In exceptional cases for which due justification shall be presented, the Data Protection Officer may allow this time limit to be extended.

### **Article 28 Entry into force/Revision**

- (1) The present data protection guidelines shall enter into force on 1 April 2014.
- (2) These guidelines can be amended as necessary, but they should be revised no later than five years after they have entered into force. Before a revised version is issued, the President shall - where required - consult with the competent statutory bodies.

Done at Munich, 19 March 2014

The President  
Benoît Battistelli

## **ANNEX 1 Specific data security requirements (Article 16 paragraph 2)**

Under Article 16, paragraph 2, appropriate technical and organisational measures shall be taken to:

1. deny unauthorised persons access to computer installations which process personal data (admittance control),
2. prevent persons employed in the processing of personal data from removing data carriers without authorisation (removal control),

3. prevent unauthorised capture as well as the unauthorised cognisance, alteration or erasure of stored data (storage control),
4. prevent unauthorised persons from using computer systems from or into which personal data are transmitted by means of automatic equipment (user control),
5. ensure that the persons authorised to use a computer system have access by means of automatic equipment solely to the personal data to which they have authorised access (access control),
6. ensure that it is possible to check and establish to which departments personal data can be transmitted by means of automatic equipment (transmission control),
7. ensure that it is possible to check and establish subsequently what personal data have been inputted into computer systems, at what time and by whom (input control),
8. ensure that personal data cannot be read, altered or erased without authorisation during transmission or during conveyance of corresponding data carriers (conveyance control).