DECISION OF THE SECRETARY-GENERAL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF THEIR PERSONAL DATA

Annex XII to the Staff Regulations

Effective Date: 28 October 2022

ANNEX XII - DECISION OF THE SECRETARY-GENERAL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF THEIR PERSONAL DATA

Article 1 – PURPOSE

1.1 This Decision sets out the rules relating to the protection of data subjects, including staff members of the Organisation, with regard to the processing of their personal data by the Organisation or on its behalf.

1.2 The Organisation is responsible for the processing of personal data of data subjects by or on behalf of the Organisation, in accordance with this Decision.

1.3 Directors shall ensure that the processing of personal data under their responsibility complies with this Decision, whether the Organisation acts as a controller or a processor.

Article 2 – DEFINITIONS

For the purposes of this Decision:

a) "**AI system**" means a machine-based system that is capable of influencing the environment by producing an outcome (prediction, recommendation, or decision) for a given set of objectives;

b) "**controller**" means the Organisation, when it determines alone or jointly with others, the purposes and means of the processing;

c) "**consent**" means any freely given, unambiguous, specific and informed indication by data subjects signifying agreement to the processing of their personal data;

d) "**director**" shall refer to directors, heads of programmes, or other staff members to whom the Secretary-General has conferred the responsibility for and executive authority over a programme of work. This term also includes the Executive Director of the International Energy Agency, the Secretary-General of the International Transport Forum, as well as other heads of programmes hosted by the Organisation;

e) "**personal data**" means any information relating to an identified or identifiable individual ("**data subject**");

f) "**personal data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, theft of, or access to, personal data transmitted, stored or otherwise processed;

g) **"processing**" means any operation which is performed on personal data, whether or not by automated means;

h) "**processor**" means a natural or legal person that processes personal data on behalf of the Organisation. The Organisation shall be considered a processor when it processes personal data on behalf of other natural or legal persons and, in such a case, all obligations of processors under this Decision shall be respected by the Organisation;

i) "**staff members**" means the officials, the temporary staff members and any other persons employed by the Organisation;

j) "**special categories of personal data**" means i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; ii) genetic data and biometric data for the purpose of uniquely identifying an individual; iii) personal data concerning an individual's health, sex life or sexual orientation; or iv) personal data concerning criminal convictions or allegations.

Article 3 – SCOPE AND RESTRICTIONS

a) This Decision applies to processing by or on behalf of the Organisation.

b) This Decision does not apply to the processing by the Organisation of personal data of staff members, which are used solely for administrative purposes within the Organisation, and contain no significant risk to privacy in this context.

c) Following consultation with the Data Protection Officer, the Organisation may restrict the application of articles 4.3, 5 and 6.4 of this Decision when this is necessary and proportionate to:

i) prevent, investigate, detect or sanction staff misconduct, in accordance with the Staff Regulations and Code of Conduct;
ii) safeguard the safety or security of the data subject or others, or the security of the Organisation's premises or its functioning;
iii) exercise or defend legal claims or respond to a request from the OECD Administrative Tribunal acting in its judicial capacity;
iv) safeguard important objectives of general public interest of a Member of the Organisation or non-Member country where the personal data at issue have been transferred by that country to the Organisation.

Such restrictions shall be lifted as soon as the circumstances that justify them no longer apply.

Article 4 – PRINCIPLES RELATING TO PROCESSING

4.1 Processing

Personal data shall be:

a) processed in a fair and transparent manner and for specified, explicit and legitimate purposes for the fulfilment of the Organisation's mission and programme of work;

b) adequate, relevant, accurate, reasonably kept up to date, and limited to what is necessary for the purposes for which the personal data are processed;

c) processed in a manner that ensures their appropriate security, including against any personal data breach, using appropriate technical or organisational measures;

d) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

4.2 Special categories of personal data

a) Processing of special categories of personal data is only permitted if:

i) Data subjects have given consent to the processing of such personal data or made such personal data manifestly public;

ii) the processing is necessary for employment with the Organisation, to safeguard the safety or security of the data subject or others, or the security of the Organisation's premises or its functioning or in relation to medical or social protection under the Organisation's Staff Regulations or under national schemes (including for health expenses coverage or the payment of family or social benefits);

iii) the processing is necessary to exercise or defend legal claims or respond to a request from the OECD Administrative Tribunal acting in its judicial capacity;

iv) the processing is necessary for scientific, historical or economic research purposes, statistical purposes, archiving purposes, policy formulation and implementation and is not intended to have any impact, direct or indirect, on the data subject; or

v) the processing is based on an agreement under international law or a binding decision of the OECD Council or another competent body.

b) In the cases mentioned in paragraph a) above, processing shall be proportionate to the purpose and appropriate safeguards of the rights, freedoms and legitimate interests of the data subjects, including in particular security measures consistent with this Decision, shall be taken by the controller.

4.3 Processing using an AI system

When the processing involves the use of an AI system to produce an outcome that affects data subjects, the controller shall provide data subjects with plain and easy-to-understand information on the factors and the logic that serve as the basis for the outcome. Data subjects adversely affected by an outcome involving an AI system have the right to challenge the outcome with the controller, in particular on grounds of inaccuracy or bias.

Article 5 – RIGHTS OF DATA SUBJECTS

5.1 Transparency and information

a) The controller shall provide information on the processing and its purpose(s) to the data subjects, as well as any amendment made to such processing, which shall be set out in a concise, transparent, intelligible and easily accessible form and made available through appropriate means.

b) The information shall include:

i) contact details of the controller;

ii) contact details of the Data Protection Officer;

iii) contact details of the Data Protection Commissioner;

iv) purposes of the processing;

v) the recipients or categories of recipients of the personal data;

vi) where applicable, the fact that the controller intends to transfer personal data outside the Organisation;

vii) the period for which the personal data will be stored, or if that is not possible, the reasons why no such period is fixed;

viii) any external storage location; and

ix) the existence of the right to request access, rectification, erasure, object to processing of personal data and to submit claims.

c) Paragraphs a) and b) above shall not apply if the provision of such information proves impossible, would involve a disproportionate effort, or is likely to render impossible or seriously impair the achievement of the objectives of the processing. In such cases, the controller takes appropriate measures to protect the data subjects' rights and freedoms and legitimate interests.

5.2 Right of access

a) Data subjects have the right to obtain from the controller confirmation as to whether their personal data are being processed, and, where that is the case, to have access to these.

b) One copy of the requesting data subject's personal data undergoing processing shall be made available to him/her, free of charge. Where the data subject makes the request by electronic means, the information shall be provided in a commonly used electronic form.

c) The right to obtain the copy referred to above shall not adversely affect the rights and freedoms of others.

5.3 Right to rectification and erasure

a) Data subjects have the right to obtain from the controller the rectification or completion of inaccurate personal data concerning them.

b) Data subjects have the right to obtain from the controller the erasure of their personal data where:

i) such data are no longer necessary in relation to the purposes for which they were processed;

ii) their personal data have been processed in contradiction with this Decision;

iii) the data subject withdraws the consent on which the processing is based.

c) Paragraph b) above does not apply to the extent that processing is necessary for:

i) scientific, historical or economic research purposes, statistical purposes, archiving purposes or policy formulation and implementation, in so far as the erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;

ii) exercising or protecting the rights of freedom of expression and information;

iii) reasons of public interest in the area of public health and security.

5.4 Right to object

Data subjects have the right to object to the processing of their personal data on the grounds that such processing is not necessary for the performance of tasks carried out in the exercise of the Organisation's mission and programme of work. The controller shall consider the objection, and if well-founded shall cease to process the personal data.

Article 6 – IMPLEMENTATION FRAMEWORK FOR PROCESSING

6.1 Accountability

a) The controller shall implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the requirements of this Decision, and be able to demonstrate that this is the case.

b) The controller and, where applicable, the processors, shall maintain a record of any processing under their responsibility. Such record shall include information related to the processing activities as set out in article 5.1 above.

6.2 Prior consultations and data protection risk assessment

a) Prior to a new or amended processing, the controller shall carry out a risk assessment of the impact of the envisaged processing on the protection of personal data (data protection risk assessment) and inform the Data Protection Officer.

b) Where a data protection risk assessment indicates that the processing may result in a high risk for the protection of personal data, the controller shall consult the Data Protection Officer. When so consulted, the Data Protection Officer provides written advice to the controller, including on safeguards that could be usefully implemented to reduce the risk. If the Data Protection Officer considers that, even with the implementation of the safeguards, the processing would result in a high risk for the protection of personal data, he/she may decide to suspend the processing pending a decision by the Data Protection Commissioner.

6.3 Data protection by design

a) The controller shall implement appropriate technical and organisational measures that are designed to implement this Decision, both at the time of the determination of the means for processing and that of the processing itself. For that purpose, they shall take into account the data protection risk assessment, the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the likelihood and severity of the risks to rights, freedoms and legitimate interests of data subjects posed by the processing.

b) The controller shall also implement appropriate technical and organisational measures for ensuring that, by default, only personal data necessary for each specific purpose of the processing are actually processed.

6.4 Personal data breach

a) The controller and, where applicable, processors, shall notify the Data Protection Officer of any personal data breach as soon as possible after its discovery.
b) The notification, which shall be in writing, shall include the facts relating to the personal data breach, its likely effects and the remedial action taken or planned. Where the notification occurs more than 72 hours after the discovery, the reasons for delay shall be provided as well.

c) Where the personal data breach is likely to adversely affect data subjects, the controller shall notify the Data Protection Commissioner without undue delay, as well as affected data subjects unless this would involve disproportionate effort.

6.5 Transfers of personal data outside the Organisation

a) Personal data may be transferred outside the Organisation under the conditions set out in this article and following consultation with the Data Protection Officer. Any onward transfers shall be subject to the same conditions, and only permitted for purposes that are compatible with the purpose for which the personal data were initially transferred.

b) Prior to the transfer, the controller shall ensure that the recipient of the personal data commits to safeguards that ensure a level of protection in line with this Decision, including, in particular, effective data subject rights and legal remedies. Such safeguards shall be proportionate to the risks to data subjects presented by the transfer, taking into account the nature of the data and the purpose and context of the processing.

c) Safeguards pursuant to paragraph b) above may result from:

(i) contractual clauses or provisions inserted in other written arrangements;

(ii) a decision of the OECD Council or another competent body that is binding upon the recipient of the personal data and the controller;

(iii) other mechanisms as may be established in specific rules adopted under article 10(b) of this Decision.

d) In the absence of safeguards pursuant to paragraph (b) above, the transfer of personal data outside the Organisation is only permitted where one of the following applies:

(i) data subjects have given their consent to the transfer, having been informed of the transfer and the related risks;

(ii) the transfer is necessary to safeguard the safety or security of the data subject or other persons, or the security of the Organisation’s premises or its functioning;

(iii) the transfer is necessary for the exercise or defence of legal claims or to respond to a request from the OECD Administrative Tribunal acting in its judicial capacity.

6.6 Processors

The controller shall ensure that processors (and any subprocessors) provide guarantees to the Organisation on the implementation of appropriate technical and organisational measures aimed at ensuring that the processing will meet the requirements of this Decision. Such guarantees shall be provided through contractual clauses or provisions inserted in other written arrangements between the controller and the processor. The engagement of subprocessors by the processor is subject to prior written authorisation by the controller.

Article 7 – DATA PROTECTION OFFICER

7.1 The Data Protection Officer is an expert with knowledge of data protection regulations, policies and practices, who shall be appointed as an official by the Secretary-General.

7.2 a) The Data Protection Officer reports directly to the Secretary-General. He/she performs his/her duties in a fully neutral manner and in full independence.

b) As required, the Data Protection Officer shall consult with the Office of the Secretary-General and the Office of the Executive Director on matters relating to his/her functions as set out in article 7.4 below.

7.3 The Data Protection Officer shall protect information of a confidential nature that has come to his/her knowledge in the performance of his/her functions.

7.4 The Data Protection Officer shall perform the following responsibilities, inter alia, he/she shall:

a) provide information and advice to the controller and, where applicable, processors, regarding this Decision;

b) promote awareness among staff members regarding their responsibilities in relation to the protection of personal data and provide for their training in this respect;

c) provide information and advice to data subjects regarding all issues related to the processing of their personal data and the exercise of their rights under this Decision;

d) take measures to ensure compliance with this Decision;

e) on his/her own initiative or on request, verify any processing;

f) decide on the temporary suspension of a processing in case of high risks for the protection of personal data and immediately inform the Data Protection Commissioner of any such decision;

g) provide the Data Protection Commissioner with: i) his/her views on any data subjects' claims alleging breach of this Decision; ii) relevant documents and/or information on the claim, personal data and/or processing concerned;

h) cooperate with the Data Protection Commissioner and act as his/her contact point on issues relating to processing.

7.5 The Secretary-General may appoint a Deputy Data Protection Officer, who shall perform, under the same conditions, the responsibilities of the Data Protection Officer in the event of his/her absence.

Article 8 – DATA PROTECTION COMMISSIONER

8.1 Mandate

a) The Data Protection Commissioner shall ensure and enforce the application of this Decision, in order to protect the rights, freedoms and legitimate interests of data subjects in relation to the processing.

b) The Data Protection Commissioner is appointed by the Secretary-General, among persons having expert knowledge of data protection regulations, policies and practices and a recognised professional experience of personal data protection matters acquired at national or international level.

c) The Data Protection Commissioner shall be appointed for a fixed term of five (5) years, which may be renewed only once for the same duration. However, in order to ensure that a Data Protection Commissioner is always in office, the term of an incumbent Data Protection Commissioner may exceptionally be extended in case of delay in the nomination of a successor to this office. The period covered by such extension(s) shall not exceed a total period of twelve (12) months. The Data Protection Commissioner may only be dismissed by the Secretary-General if he or she no longer fulfils the conditions required for the performance of his or her duties or if he or she is guilty of serious misconduct.

d) Any person who has served as Data Protection Commissioner shall not be employed in any capacity by the Organisation nor enter into any contractual relationship with the Organisation for a period of twelve (12) months from the date of the cessation of his/her mandate.

e) The detailed terms and conditions for the performance of the Data Protection Commissioner's duties are laid down by the Secretary-General and shall prohibit the Commissioner from engaging in other tasks and duties that create a conflict of interest.

f) The Data Protection Commissioner performs his/her mandate independently and in a fully neutral manner. The Data Protection Commissioner shall neither seek nor take instructions from anyone. He/she shall have the resources necessary to exercise the mandate effectively and may inform the Secretary-General of any difficulties encountered.

g) In the performance of his/her mandate, the Data Protection Commissioner shall enjoy the same privileges and immunities as those accorded to experts on mission by virtue of the additional protocols to the Convention on the OECD. In particular, he/she may not be subject to any constraints, nor be compelled to be a witness in procedures carried out outside the Organisation, with regard to events or documents which have come to his/her knowledge in the performance of his/her mandate.

8.2 Responsibilities

The Data Protection Commissioner shall primarily:

a) provide advice on the optimal implementation of this Decision, taking account of new developments and challenges and best international practice;

b) investigate and review, with the assistance of the Data Protection Officer, the claims submitted to him/her alleging breach of this Decision and submit his/her final conclusions to the Secretary-General;

c) notify the controller and, where applicable, the processors, of an infringement of this Decision;

d) communicate to the Secretary-General, as necessary, general comments aimed at ensuring the protection of personal data;

e) submit an annual activity report to the Secretary-General. This report shall provide an overview of the state of data protection within the Organisation, including relevant initiatives to raise awareness and implement the requirements of this Decision. The report shall also summarise any claims submitted to the Data Protection Commissioner during the year and their results, without identifying the data subject(s)

concerned. This report shall be shared with all staff members and posted on the Organisation's intranet and internet.

8.3 Powers

8.3.1 The Data Protection Commissioner shall have the following investigative powers:

a) to order the controller, and, where applicable, the processors, to provide any information he/she requires for the performance of his/her mandate;

b) to carry out investigations related to any processing;

c) to obtain from the controller and, where applicable, the processors, access to: i) all personal data and to all information available to them; and ii) their premises and devices necessary for the performance of his/her mandate.

8.3.2 The Data Protection Commissioner shall have the following corrective powers:

a) to order the controller and, where applicable, the processors, to:

i) comply with the data subjects' rights pursuant to this Decision;

ii) bring processing into compliance with this Decision;

iii) communicate a personal data breach to the data subjects concerned, and where the data subjects are staff members, to the Head of Human Resources Management;

iv) rectify or erase personal data or restrict processing and notify such actions to recipients to whom the personal data have been disclosed.

b) to decide to lift or maintain the suspension of the processing decided by the Data Protection Officer in accordance with article 7.4 f) above and immediately informs the Data Protection Officer and the controller of any such decision;

c) to impose a limitation, including a ban, on the processing of certain personal data.

Article 9 – SETTLEMENT OF CLAIMS

9.1 When investigating claims submitted by data subjects, the Data Protection Commissioner shall invite the controller and, where applicable, the processors, and the data subjects concerned, to express written views on the claims and the relevant facts and to provide evidence or views on evidence already at hand.

9.2 After reviewing the claim, the evidence and any written comments submitted by the controller, and where applicable, the processors, and the data subjects concerned, the Data Protection Commissioner may order or impose the measures set out in article 8.3.2 above.

9.3 The reasoned conclusions of the Data Protection Commissioner are communicated to the Secretary-General within two months of the submission of the claim. These conclusions are binding and final, except where there is an obvious material error.

9.4 The Secretary-General shall take a decision in accordance with the conclusions of the Data Protection Commissioner and notify it, together with the conclusions of the Data Protection Commissioner, to the claiming data subject, the controller, and, where applicable, processors, and the Data Protection Officer. The decision of the Secretary-General shall be notified within two weeks of the date of the Data Protection Commissioner's conclusions. A copy of this decision is sent to the Data Protection Commissioner.

9.5 The decision of the Secretary-General may only be challenged before the Administrative Tribunal by staff members and claimants to their rights, as well as persons applying for appointment in the Organisation, in accordance with Staff Regulation 22 and Annex III to the Staff Regulations applicable to officials.

9.6 To challenge the decision of the Secretary-General, data subjects who are not staff members, claimants to their rights or persons applying for appointment in the Organisation must, within four months from the date of notification of the contested decision, submit a written request to the Secretary-General for withdrawal or modification of the contested decision. If the Secretary-General denies such request or does not reply within a period of three months (implied denial of such request), data subjects may file a notice of arbitration in accordance with article 9.7 of this Decision.

9.7 Any dispute or claim arising out of a decision of the Secretary-General notified to data subjects who are not staff members, claimants to their rights or persons applying for appointment in the Organisation shall be settled by final and binding arbitration in accordance with the 2012 Arbitration Rules of the Permanent Court of Arbitration (PCA). The number of arbitrators shall be one (1). The appointing authority shall be the Secretary-General of the PCA. The language to be used in the arbitral proceedings shall be English. The place of arbitration shall be Paris (France).The law applicable to this arbitration shall be the provisions of this Decision. The arbitration award shall be final and binding on both the Organisation and the claimant.

9.8 Notice of arbitration given under article 9.7 must be filed with the Organisation and the International Bureau of the PCA within six months from the date of notification of the denial by the Secretary-General of the written request submitted in accordance with article 9.6 above or from the date of the implied denial of such request, whichever occurs first.

Article 10 – PUBLICITY AND AMENDMENTS

a) This Decision, which replaces the Decisions of July 1992, September 2001, September 2005 and May 2019, shall be published on the Organisation's Intranet and Internet sites and shall enter into force when so published.

b) The Secretary-General may adopt specific rules and/or guidelines on any matter related to this Decision, following consultation with the Data Protection Commissioner and the Data Protection Officer. All references to 'this Decision" shall be deemed to include such rules and guidelines.

c) This Decision shall be reviewed at least every five (5) years after entry into force and may be amended at any time.

* * *