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: 3 May 2019

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 individuals, 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 implementation of any processing of Personal Data by the Organisation is subject to compliance with this Decision and any other relevant rules of the Organisation adopted for its implementation.

1.3 The Organisation is responsible for the processing of Personal Data of individuals by or on behalf of the Organisation, in accordance with this Decision and any other relevant rules of the Organisation adopted for its implementation.

Article 2 – DEFINITIONS

a) "**Personal Data**" means any information relating to an identified or identifiable individual;

b) "**Processing**" means any operation which is performed on Personal Data, wholly or partly, by automated means;

c) "**Consent**" of individuals to Processing referred to in this Decision and any other relevant rules of the Organisation adopted for its implementation means any freely given, unambiguous, specific and informed indication signifying agreement to the Processing of Personal Data relating to them or to individuals on whom they exercise legal authority. This consent shall be given in an intelligible and easily accessible form, using clear and plain language and only applies to the specific Processing for which it is collected;

d) "**Staff members**" means, for the purpose of the Decision, the officials, the temporary staff members and any other persons employed by the Organisation;

e) The **"Coordinators"** are the Organisation's staff members who determine, alone or jointly with others, the purposes and means of the Processing, on behalf of the Organisation;

f) The "**Processors**" are individuals or institutions external to the Organisation, including other international organisations, which process Personal Data on behalf of the Organisation;

g) "**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;

h) "**Profiling**": 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 significantly affects him or her.

Article 3 – SCOPE

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

b) This Decision does not apply to the processing by the Organisation of Personal Data:

i) of staff members and members of the delegations of Member countries, which are used solely for administrative purposes within the Organisation, and contain no significant risk to privacy in this context, namely the surname, first name, grade, functions, professional physical and e-mail addresses, professional telephone numbers, preferred official working language and photographs;

ii) of staff members in relation to the prevention, investigation, detection or sanction of any kind of misconduct, which are processed in accordance with the Staff Regulations and Code of Conduct applicable to them;

iii) for the purposes of the prevention, investigation, detection or sanction of action presenting a safety or security risk for the Organisation's staff members and visitors, which are processed in accordance with the relevant policies, guidelines and decisions taken by the Secretary-General;

iv) for the purposes of the prevention, investigation, detection or sanction of action presenting a safety or security risk for the Organisation's assets or reputation;

v) for the exercise or defence of legal claims or in follow-up to a request from the OECD Administrative Tribunal acting in its judicial capacity.

Article 4 – PRINCIPLES RELATING TO PROCESSING

4.1 Processing

Personal Data shall be:

a) processed in a transparent manner and for specified, explicit and legitimate purposes for the delivery of the Organisation's mission and programme of work, in accordance with this Decision and any other relevant rules of the Organisation adopted for its implementation;

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 to the extent reasonably possible;

d) kept for no longer than is necessary for the purposes for which the Personal Data are processed.

4.2 Sensitive Personal Data

a) The Processing of the following Personal Data is prohibited:

i) Personal Data revealing ethnic origin, political opinions, religious or philosophical beliefs, trade union membership;

ii) Personal Genetic Data and Personal Biometric Data for the purpose of uniquely identifying individuals;

iii) Personal Data concerning health and individuals' sex life or sexual orientation.

b) Paragraph a) above is not applicable if:

i) individuals have given consent to the processing of such Personal Data or made such Personal Data manifestly public. The Coordinators may be asked to demonstrate that the individuals have consented to the processing of such Personal Data;

ii) the Processing is necessary for employment with the Organisation, for the management of safety or digital security risk to the Organisation, its staff and visitors 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 for scientific, historical or economic research, statistical or related archiving purposes, for the delivery of the Organisation's mission and programme of work.

c) In the cases mentioned in paragraph b) above, appropriate safeguards of the rights and interests of the individuals shall be taken by Coordinators.

4.3 Automated Processing, including profiling

a) A decision based solely on automated Processing, including profiling, which produces legal effects concerning individuals or significantly affects them, shall be prohibited.

b) Paragraph a) above shall not apply if the Processing:

i) is necessary for the Organisation to choose to enter into a contract with providers or staff members;

ii) is necessary for the Organisation to ensure follow-up regarding the performance of contracts and staff members;

iii) is expressly authorised by the rules of the Organisation provided that they lay down suitable measures to safeguard the individuals' rights and freedoms and legitimate interests, including the right to obtain human intervention on the part of the Organisation, to express his/her point of view and to contest the result of the Processing; or

iv) is based on the individuals' explicit consent.

Article 5 – RIGHTS OF INDIVIDUALS

5.1 Transparency and Information

a) Coordinators shall provide information on the Processing and its purpose(s) to the Data Protection Officer, as well as any amendment made to such Processing, which shall be set out in a concise, transparent, intelligible and easily accessible form.

b) The Data Protection Officer shall make this information available to individuals through appropriate channels on the intranet and/or internet websites of the Organisation, as appropriate and in a manner that protects the individual's rights and freedoms and legitimate interests. The Data Protection Officer shall also make this information available to specific individuals, on their request.

c) The information shall include:

i) contact details of the Coordinators;

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 Organisation intends to transfer Personal Data to a Member of the Organisation or a non-Member country or another international organisation or third party;

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;

ix) and the existence of the right to request access, rectification or erasure of Personal Data and to submit claims.

d) Information need not be provided if the provision of such information proves impossible or would involve a disproportionate effort. In such cases, the Organisation takes appropriate measures to protect the individuals' rights and freedoms and legitimate interests to the extent reasonably possible.

5.2 Right of access

a) Individuals have the right to obtain from the Coordinators confirmation as to whether their Personal Data are being processed, and, where that is the case, to have access to these. Requests to this effect shall be addressed to the Data Protection Officer.

b) One copy of the requesting individual's Personal Data undergoing Processing is made available to him/her, free of charge. Where the individual makes the request by electronic means, the information is 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) Individuals have the right to obtain from the Coordinators the rectification or completion of inaccurate Personal Data concerning them.

b) Individuals have the right to obtain from the Organisation 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 and any other relevant rules of the Organisation adopted for its implementation.

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

i) scientific, historical and economic research, statistical or archiving purposes, for the delivery of the Organisation's mission and programme of work, 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

Individuals have the right to submit a request to the Coordinators objecting to the Processing of their Personal Data, when such Processing is not necessary for the performance of tasks carried out in the exercise of the Organisation's official activities or in the framework of its mission.

5.5 Right to Data Portability

Individuals have the right to obtain from the Coordinators that their Personal Data be transmitted to them or to any person or institution they designate, in a structured, commonly used and machine readable format where available, where technically feasible and on the condition that they provide adequate transmission information and cover any costs involved in advance.

Article 6 – IMPLEMENTATION FRAMEWORK FOR PROCESSING

6.1 Accountability

a) Coordinators shall implement appropriate technical and organisational measures to ensure that Processing is performed in accordance with the requirements of this Decision and any other relevant rules of the Organisation adopted for its implementation, and be able to demonstrate that this is the case.

b) The Organisation does not restrict the transborder flows of Personal Data towards its Member countries, non-Member countries and other international organisations, where (i) these countries or organisations substantially observe this Decision and any other relevant rules of the Organisation adopted for its implementation or (ii) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by these countries or organisations, to ensure a continuing level of protection consistent with this Decision and any other relevant rules of the Organisation adopted for its implementation.

c) Any restriction to transborder flows of Personal Data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the Processing. For example, the Organisation may impose restrictions in respect of certain categories of Personal Data for which this Decision and any other relevant rules of the Organisation adopted for its implementation include specific provisions in view of the nature of those data.

d) Coordinators shall consult with the Data Protection Officer and the Data Protection Commissioner where they intend to proceed with transborder flows of Personal Data or to restrict such transborder flows.

6.2 Prior Consultations and Data Protection Risk Assessment

a) Coordinators shall inform the Data Protection Officer of the creation of, or amendment to, any Processing.

b) Prior to a new Processing, Coordinators shall carry out a risk assessment of the impact of the envisaged Processing on the protection of Personal Data (Data Protection Risk Assessment). They may seek advice from the Data Protection Officer as to the optimal management of the risk.

c) Where a Data Protection Risk Assessment indicates that the Processing may result in a high risk for the protection of Personal Data, Coordinators shall consult the Data Protection Officer. When so consulted, the Data Protection Officer provides written advice to the Coordinators, including on safeguards that could be usefully implemented to reduce the risk. If the Data Protection Officer considers that, even with the implementation of 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) Coordinators shall implement appropriate technical and organisational measures which 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 for rights, freedoms and legitimate interests of individuals posed by the Processing.

b) Coordinators shall also 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 actually processed. They may seek advice from the Data Protection Officer in that regard.

6.4 Security

6.4.1 Security of Personal Data

Coordinators and, where applicable, Processors shall treat the risk by implementing appropriate technical and organisational measures, in close liaison with the Organisation's internal experts, to ensure a level of security reasonably appropriate to the risk.

6.4.2 Personal Data Breach

a) Coordinators and, where applicable, Processors, shall notify any Personal Data Breach, its nature and circumstances to the Data Protection Officer and the Data Protection Commissioner, within 48 hours of its discovery.

b) The documentation prepared by Coordinators and, where applicable, Processors, on any Personal Data Breach shall include the facts relating to the Personal Data Breach, its likely effects and the remedial action taken, if any. Such documentation shall be submitted to the Data Protection Officer and the Data Protection Commissioner.

c) Coordinators and, where applicable, Processors, shall also communicate the Personal Data Breach to the individuals concerned, without undue delay and through appropriate channels, unless this would involve disproportionate effort. In the latter case, they shall inform the Data Protection Officer and the Data Protection Commissioner of the absence of notification to the individuals concerned and its rationale. The Data Protection Commissioner may nevertheless require them to proceed with the notification where he/she considers that the Personal Data Breach is likely to result in a high risk for the individuals concerned or for others. In such a case, the Data Protection Commissioner determines the modalities for such notification.

6.4.3 Processors

Processors shall 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 and any other relevant rules of the Organisation adopted for its implementation.

6.4.4 Record of processing activities

Coordinators and, where applicable, 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.

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 which 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 Coordinators and, where applicable, Processors, regarding this Decision and any other relevant rules of the Organisation adopted for its implementation;

b) promote awareness of Coordinators and staff members in relation to the protection of Personal Data and provide for their training in this respect;

c) provide information and advice to individuals regarding all issues related to the Processing of their Personal Data and the exercise of their rights under this Decision and any other relevant rules of the Organisation adopted for its implementation;

d) take measures to ensure compliance with this Decision and with other relevant rules of the Organisation adopted for its implementation;

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 individuals' claims alleging breach of this Decision or of any other relevant rules of the Organisation adopted for its implementation; 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;

i) be consulted by the Data Protection Commissioner and provide him/her with any information and assistance required.

Article 8 – DATA PROTECTION COMMISSIONER

8.1 Mandate

a) The Data Protection Commissioner shall ensure and enforce the application of this Decision and any other relevant rules of the Organisation adopted for its implementation, in order both to protect the rights, freedoms and legitimate interests of individuals in relation to the Processing and to facilitate the free flow of Personal Data.

b) The Data Protection Commissioner is nominated 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 within a national or international administration.

c) The Data Protection Commissioner shall be nominated 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.

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.

f) The Data Protection Commissioner performs his/her mandate independently and in a fully neutral manner, and shall have the resources necessary to exercise it effectively. He/she may inform the Secretary-General and his/her office of the difficulties encountered in the performance of his/her mandate.

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) assist and advise Coordinators and, where applicable, Processors, on the required analysis of the data protection risk and its treatment;

b) investigate and review, with the assistance of the Data Protection Officer, the claims submitted to him/her alleging breach of this Decision and any other relevant rules of the Organisation adopted for its implementation and submit his/her final conclusions to the Secretary-General;

c) notify the Coordinators and, where applicable, the Processors, of an infringement of this Decision or any other relevant rules of the Organisation adopted for its implementation;

d) communicate to the Secretary-General, each time it is necessary, general comments aimed at ensuring the protection of Personal Data;

e) submit an annual activity report to the Secretary-General. This report shall summarise the main areas where he/she has intervened over the previous year, his/her actions in terms of awareness raising and the number of claims treated and their overall results. This report shall not permit the identification of individuals who asked the Data Protection Commissioner to intervene or submitted a claim to the Data Protection Commissioner. 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 Coordinators, 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 Coordinators 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 Coordinators and, where applicable, the Processors, to:

i) comply with the individuals' rights pursuant to this Decision and any other relevant rules of the Organisation adopted for its implementation;

ii) bring Processing into compliance with this Decision and any other relevant rules of the Organisation adopted for its implementation;

iii) communicate a Personal Data Breach to the individuals concerned, and where the individuals 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 Coordinators of any such decision;

c) to impose a limitation, including a ban, on processing of certain Personal Data.

Article 9 – SETTLEMENT OF CLAIMS

9.1 When investigating claims submitted to him/her by individuals, the Data Protection Commissioner shall invite the Coordinators and, where applicable, the Processors, and the individuals 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 Coordinators, and where applicable, the Processors, and the individuals 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. 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 individual, the Coordinators, and, where applicable, Processors, and the Data Protection Officer. 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 Any dispute or claim arising out of a decision of the Secretary-General notified to individuals who are not staff members, claimants to their rights or persons applying for appointment in the Organisation, and which cannot be settled amicably within two (2) months of the receipt of the claim by the Secretary-General, shall be settled by final and binding arbitration in accordance with the Permanent Court of Arbitration Optional Rules for Arbitration between International Organisations and Private Parties, as in effect on the date of the receipt of the claim. The number of arbitrators shall be one (1). The appointing authority shall be the Secretary-General of the Permanent Court of Arbitration. The language to be used in the arbitral proceedings shall be English. The place of arbitration shall be Paris (France).The applicable law to this arbitration shall be the provisions of this Decision and any other relevant rules of the Organisation adopted for its implementation. The arbitration award shall be final and binding on both the Secretary-General and the claimant.

Article 10 – PUBLICITY AND AMENDMENTS

a) This Decision, which replaces the Decisions of July 1992, September 2001 and September 2005, 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, upon recommendation of the Data Protection Commissioner and/or the Data Protection Officer.

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

* * *