ESA
Director General's Office

Distribution: All staff

ESA/ADMIN/IPOL-LEGI(2018)01
Paris, 5 February 2018
(Original: English)

ESA Unclassified – Releasable to the public

POLICY ON PERSONAL DATA PROTECTION

1. INTRODUCTION

In the performance of its mission, the Agency collects and has to process certain Personal Data concerning various individuals, in particular Staff Members or Contractor Personnel. These Personal Data may be collected by the Agency or made available to the Agency by the individuals themselves or by third parties, located in several jurisdictions.

The Agency, while not being subject to national or international laws on Personal Data protection, wants to ensure a high level of protection of Personal Data and, by doing so, to preserve the dignity and privacy of the concerned individuals.

To that effect, the ESA Council adopted a Resolution on a "Personal Data Protection Policy" setting forth the principles of Personal Data Protection at ESA and mandating the Director General to adopt a Policy on Personal Data Protection ("Policy") implementing the said principles and establishing an appropriate governance scheme the latter to be composed of an independent Data Protection Supervisory Authority, an internal Data Protection Committee and a Data Protection Officer.

2. POLICY

In order to ensure a high level of protection of Personal Data concerning individuals and in particular Agency's Staff Members and Contractor Personnel, it is the Agency's policy to:

- adopt a structured framework to effectively ensure the protection and safeguard of Personal Data processed or disclosed by, on behalf of, or to the Agency,

- increase awareness and responsibility of Staff Members with respect to Personal Data protection,

- establish governance, including functions and bodies (e.g. Data Protection Officer, Data Protection Supervisory Authority, Data Protection Committee) and operations necessary for the effectiveness of Personal Data protection.

3. DEFINITIONS

For the purpose of this Policy and its Annex, the following terms are defined as follows:

Adequate Level of Protection means a level of protection of Personal Data adequate in the consideration of this Policy, as recognised:

(i) by decision(s) taken by the Director General upon recommendation of the Data Protection Officer ;

(ii) by this Policy to the following countries and international organisations:

a. the Member States of the Agency, the European Union, its institutions and bodies as well as the States which are members of the European Union; and,

b. the countries and other international organisations recognised by the European Commission as offering an adequate level of protection under the European Union's legal framework.

Contractor means the natural or legal person who has entered into a Contract with the Agency and which, with regard to Personal Data, acts either as a Data Controller or as a Data Processor.

Contractor Personnel means the personnel engaged by the Contractor (including that of its subcontractors) to undertake the contracted tasks and who is acting under the Contractor's responsibility.

Consent means the informed permission expressed by a Data Subject relating to the Processing of his/her Personal Data.

Data Controller means any natural or legal person who makes the decision, alone or conjointly, to Process Personal Data, or commissions others to Process Personal Data on its behalf. The quality of Data Controller belongs to the Agency itself, not to the Agency's Staff Member who is materially involved in the related activities. The quality of Data Controller belongs to the Contractor itself, not to the Contractor Personnel who is materially involved in the related activities.

Data Processor means any natural or legal person, which Processes Personal Data on behalf of the Data Controller. With regard to Personal Data Processing materially operated by a Staff Member, the quality of Data Processor belongs to the Agency itself, not to the Staff Member. The quality of Data Processor belongs to the Contractor itself, not to the Contractor Personnel who is materially involved in the related activities.

Data Protection Officer means the Agency's Staff Member appointed by the Director General to perform the duties listed in Annex to this Policy or assigned to him/her by decision of the Director General.

Data Protection Committee means the consultative body established under Annex to this Policy.

Data Subject means an individual who is the subject of Personal Data.

Data Protection Supervisory Authority or *Supervisory Authority* means the independent supervisory authority in the field of Personal Data protection, established under Annex to this Policy.

Disclosure (or "transfer") of Personal Data or *Disclosure* (or *Disclose*) means any movement of Personal Data, including by copy, by moving Personal Data through a network or from one medium to another (e.g. from a computer hard disk to a server), and/or by rendering remotely accessible Personal Data.

Dispute Resolution Procedure means a process for resolving, internally or externally, differences or conflict between two or more parties, such as a litigation, arbitration, mediation or conciliation procedure.

ESA Premises means the Agency's establishments, centres and any other Agency's facilities.

Health-related Sensitive Personal Data means Personal Data relating to the physical or mental health of the Data Subject.

Incident or *Data Protection Incident* means any intentional or unintentional activity which violates the provisions set forth in this Policy.

Investigation Procedure means an process of examination or search, whether internal or external to the Agency, in order to gather facts and collect evidence.

Personal Data means any information concerning an identified or identifiable Data Subject, in this latter case provided that identification of the said Data Subject may be done without unreasonable efforts.

Personal Data Processing or *Processing* (or *Process*) means any operation or set of operations performed by electronic means on Personal Data, such as collection, recording, organisation, storage, retrieval, use, Disclosure, deletion, excluding the mere consultation.

Personal Data Recipient or *Recipient* means, in relation with a Disclosure of Personal Data, the third party (whether a natural or legal person, whether another Data Controller or Data Processor, but which is not acting under the authority of the said third party), to which Personal Data is Disclosed.

Personal Data Records means, in relation to Personal Data, records to be created and maintained by the Data Protection Officer, including concerning Personal Data Processing, requests made by Data Subjects in the exercise of their rights under this Policy, notifications, investigations, recommendations and findings related to Data Protection Incidents.

Sensitive Personal Data means Personal Data that can reveal without unreasonable efforts the racial or ethnic origins, political opinions, trade union membership, religious or philosophical beliefs, health or sexual life, genetic or biometric data, criminal convictions of a Data Subject,

4. SCOPE

This Policy protects all Personal Data, relating to any Data Subject, whether collected by the Agency or disclosed to the Agency by a third party.

For the sake of clarity, this Policy does not apply to data that are rendered anonymous in such an irreversible way that Data Subjects cannot be readily identified from the data.

Without prejudice to the specific provisions set forth in this Policy, the security principles and the security implementation standards, which are laid down in ESA Security Regulations and Directives, are applicable within their scope.

5. PRINCIPLES

The following principles concerning

i. Personal Data quality,
ii. Processing of Personal Data and Sensitive Personal Data,
iii. Disclosure of Personal Data,
iv. Data Subject's rights,
v. Safety of Personal Data,
vi. Prevention, reporting and investigation of Data Protection Incidents, and,
vii. Processing of Personal Data on behalf of the Agency

are common to all Data Subjects and shall be implemented according to the applicable Agency's procedures and guidelines.

5.1 Personal Data quality

Personal Data shall be:

i. accurate and, where necessary, kept up to date.

   To that effect, Personal Data may, at the request of the Data Subject, be erased, rectified, completed, amended, as the case may be, if, and to the extent, they are:

   a. proved to be inaccurate or incomplete, having regard to the purposes for which they are Processed, or

   b. Processed in violation with the principles referred to in Section 5.2. of this Policy,

ii. kept in a form which permits identification of the Data Subject as necessary for the purposes for which the Personal Data were collected or for which they are further Processed.

5.2 Processing of Personal Data and Sensitive Personal Data

5.2.1 *General.*

Processing of Personal Data shall be done:

i. fairly, for specified and legitimate purposes and may be further processed in a way compatible with those purposes, the compatibility being assessed by the Data Protection Officer; the foregoing conditions shall be verified taking into account, cumulatively, the circumstances under which the Personal Data are Processed, the purposes that a reasonable Data Subject would consider appropriate, and the necessity of the Processing.

The Processing is deemed fair and legitimate when it relates to :

a. the performance of an activity carried out by the Agency within its purpose and in the framework of, and in conformity with, the ESA Convention, the *"Agreement between the States Parties to the Convention for the establishment of a European Space Agency*

and the European Space Agency for the protection and the exchange of classified information" done in Paris on 19 August 2002, and the applicable rules and procedures, including ESA Security Regulations and Directives; this includes Processing necessary for the Agency's management and functioning or Investigation Procedures; or

b. compliance with a legal obligation to which the Agency is subject; or

c. a task in the frame of the Agency's cooperation with the competent authority of Member States, in order to facilitate the proper administration of justice; or

d. security; or

e. the performance of a contract concluded by the Agency within its purpose in relation with an activity carried out by the Agency in the framework of, and in conformity with, the ESA Convention and the applicable rules and procedures; or

f. the legitimate interest of the Data Subject; or

g. a purpose covered by the Consent of the Data Subject,

ii. in a not excessive manner, as necessary for the purposes for which the Personal Data were collected or for which they are further Processed; and,

iii. in conditions protecting confidentiality, integrity and safety of Personal Data, preserving the rights of the Data Subject set forth in Section 5.4 herein and conforming to instructions from the Data Controller.

When designing and selecting information technology systems, software and services for the Processing of Personal Data, compliance with the principles set forth in this Policy shall be ensured.

5.2.2. <u>*Sensitive Personal Data.*</u>

5.2.2.1 The Processing of Sensitive Personal Data is forbidden, except if :

i. it is covered by the Consent of the Data Subject; or

ii. it relates to Sensitive Personal Data which are manifestly made public by any means (for instance, social media) by the Data Subject; or

iii. it is necessary for :

(a) the protection of the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent; or

(b) Investigation Procedures; or

(c) the purposes of carrying out obligations of the Agency under the applicable staff Regulations, Rules and Instructions or Pension Rules or the provision of health or social care or the treatment or the management of health or social care systems and services; and,

(d) the protection against serious threats to security or health.

5.2.2.2 In all these cases, Processing must be done in accordance with the principles set forth in Section 5.2.1. and the Data Protection Officer shall be notified prior to the such Processing.

5.2.2.3 In addition, the Processing of Health-related Sensitive Personal Data may only be done:

a. by, or under the responsibility of, a health professional subject to the obligation of professional secrecy or an Agency Staff Member managing health care or social security services or a Contractor acting on behalf of the Agency in the field of social security; and,

b. under the generally applicable medical professional standards, as recommended by the Agency's medical advisor.

5.3 Disclosure of Personal Data

In all cases mentioned below, Personal Data shall be Disclosed in compliance with the general Processing principles set forth in Section 5.2.

5.3.1. *Disclosure within the Agency*

i. Disclosure within the Agency shall be done freely in line with the Policy, regardless of the country where the Data Recipient within the Agency is located.

ii. Disclosure of Personal Data to identified entities in charge of the management of the Agency's Pension Scheme within an international organisation, which is not subject to the national law of a Member State, shall be considered as a Disclosure within the Agency.

5.3.2. *Disclosure outside the Agency*

i. The Data Protection Officer shall be notified prior to any Disclosure outside the Agency, according to the applicable Agency's procedures and guidelines.

ii. Disclosure of Personal Data to Data Recipients located outside the Agency is authorised provided that the concerned country or the international organisation (others than the international organisations mentioned under Section 5.3.1 ii.) is recognised as providing an Adequate Level of Protection.

Such recognition may at any time be suspended or withdrawn by the Director General, upon recommendation of the Data Protection Officer in order to safeguard the Agency's interests or those of the Data Subjects.

iii. Notwithstanding the above and without prejudice to the other provisions of this Policy, Personal Data can however be Disclosed to Data Recipients located in a country or international organisation not offering an Adequate Level of Protection, if one of the following occurs:

a. the concerned Data Subject has given his/her Consent to the proposed Disclosure;

b. the Disclosure is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request;

c. the Disclosure is necessary for the conclusion or the performance of a contract entered into in the interest of the Data Subject between the Agency and a third party;

d. the Disclosure is necessary or legally required on important grounds of public interest, or for any Investigation or Dispute Resolution Procedure;

e. the Disclosure is necessary in order to protect the vital interests of the Data Subject or that of the Agency; and,

f. the Disclosure has been previously authorised by the Data Protection Officer under Section I vii. of the Annex following an impact assessment to be performed by the relevant organisational entity of the Agency and is done with the adequate safeguards with respect to the protection of the Personal Data and Data Subject's rights; such safeguards may in particular result from appropriate contractual clauses.

5.4 Data Subject's rights

5.4.1 The following rights of the Data Subjects shall be recognised and protected by the Agency:

i. The right to be informed, in a transparent manner, as reasonably practicable, about:

a. the identity of the Data Controller and contact details of the Data Protection Officer;

b. the purpose of the Data Processing, in case his/her Personal Data are Processed;

c. the Data Recipients to whom his/her Personal Data shall be Disclosed;

d. the existence of the rights mentioned in this Section 5.4.1 paragraphs ii., iii and iv. below;

e. the time-limits, for storing the Personal Data (or the criteria used to determine the time-limits) as decided, in compliance with Section 5.2, by the Director General upon proposal of the Data Protection Officer (following consultation of the Department in charge of personnel matters, the Record Manager and other relevant Departments); and,

f. the practical modalities of exercising the rights set forth in this Section 5.4.1 paragraphs ii., iii. and iv.

ii. The right for every Data Subject at any time to make reasonable request for access to the Personal Data relating to him/her, provided that the Data Subject demonstrates legitimate grounds; in addition, in the case of Health-related Sensitive Personal Data, the conditions under which access is granted are those corresponding to generally applicable medical professional standards, as recommended by the Agency's medical advisor;

iii. The right for every Data Subject to have his/her Personal Data erased, rectified, completed, amended as per the conditions set under Section 5.1. i. of this Policy;

iv. The right for every interested Data Subject to lodge a complaint before the Supervisory Authority in case the former demonstrates or has serious reasons to believe that a Data Protection Incident occurred in relation with his/her Personal Data, following a decision of the Agency (e.g. Data Protection Officer). Such complaint shall be lodged in accordance with the Rules of Procedure of the Supervisory Authority.

5.4.2 The right of information under Section 5.4.1i. and the right of access under Section 5.4.1 ii. shall not apply :

a. where and insofar as the Data Subject is already in possession of the information;

b. for the right of information, when processing of Personal Data is necessary for any Investigation or Dispute Resolution Procedure;

c. for the right of access, where and insofar such access would conflict with an Investigation Procedure concerning the Data Subject.

5.5 Personal Data safety

The Agency shall take any appropriate measures against the risks of loss of Personal Data as well as against unauthorised access, destruction, use, modification or Disclosure of Personal Data, in particular for what concerns Sensitive Personal Data.

Such appropriate measures may include technical (e.g. use of prevention software, products or services) or organisational measures. In case of Disclosure of Personal Data to a Contractor, the Agency shall require the Contractor to assume obligations consistent with the terms set of this Policy and of any safety procedures adopted in the implementation of this Policy.

5.6 Prevention, reporting and investigation of Data Protection Incidents

To ensure effective protection of Personal Data, a high priority is placed on prevention and resolution of Data Protection Incidents by:

i. assigning clear roles and responsibilities within the Agency in relation with Personal Data protection matters;

ii. adopting, enhancing and implementing prevention and emergency measures;

iii. putting in place controls and audits; and,

iv. investigating, mitigating the consequences of and, to the extent possible, remedying the reported or detected Data Protection Incidents.

5.7 Processing of Personal Data on behalf of the Agency

The Agency shall only assign the responsibility of Processing of Personal Data to a Data Processor if the latter provides adequate warranties of compliance with the level of protection of the Personal Data set forth by this Policy as well as in the applicable procedures, and takes commitments consistent therewith.

6. GOVERNANCE

This Policy, under its Annex, establishes the Agency's Personal Data protection governance based on the roles and responsibilities of the Agency's:

i. Data Protection Officer;

ii. Data Protection Supervisory Authority (served by a Registrar); and,

iii. Data Protection Committee.

7. ROLES AND RESPONSIBILITIES

7.1 Data Protection Officer

The Data Protection Officer (including his/her deputy) is responsible for discharging the duties assigned to him/her under Annex to this Policy and to perform any other responsibilities assigned to him/her by the Director General.

7.2 Data Protection Supervisory Authority (The Supervisory Authority)

The Supervisory Authority is competent to examine Incidents and review decisions of the Agency in the field of Personal Data Protection, upon a complaint lodged by a Data Subject in accordance with Section 5.4.1 iv. of this Policy and the Rules of Procedure referred to in Annex. Annex to this Policy details in particular its composition and appointment, its duties, its status and refers also to its Registrar.

7.3 Data Protection Committee

The Data Protection Committee, upon request of the Data Protection Officer, is responsible for providing its inputs, opinions or recommendations in application of Annex to this Policy.

7.4 Director General

The Director General oversees the implementation of the Policy and decides :

i. On the appointment or termination of appointment as Data Protection Officer and deputy, as per Section I of the Annex herein;

ii. On the resources dedicated to the implementation of this Policy;

iii. On proposals, recommendations or requests made by the Data Protection Officer in the performance of his/her duties, including but not limited in relation with Processing of Sensitive Personal Data, Disclosure of Personal Data outside the Agency, the recognition of the Adequate Level of Protection etc.

7.5 The Department in charge of Legal affairs

The Department in charge of Legal affairs shall advise the Data Protection Officer, Data Protection Committee and Director General for questions on the interpretation and application of the provisions and derived practices of this Policy and more generally on the evolutions of the Agency's Data Protection framework.

7.6 The Department in charge of personnel matters

The Department in charge of personnel matters shall, within its area of responsibility:

i. implement actions and report to the Data Protection Officer and Director General in the application of this Policy with respect to the Staff Regulations, Rules and Instructions and associated policies concerning Staff Members;

ii. provide regular Data Protection awareness training to Staff Members in coordination with the Data Protection Officer; and,

iii. support the Data Protection Officer when answering Staff Member or other affected Data Subject's questions and complaints concerning the Processing of their Personal Data.

7.7 The Department in charge of the corporate information technology

The Department in charge of corporate information technology shall take the necessary measures in order to:

i. implement this Policy and advise on the technical solutions to enforce this Policy across the Agency; and,

ii. on security aspects, mitigate the risks of technologies used by the Agency for the protection of the legitimate interests and rights of Data Subjects.

7.8 The Department in charge of Procurement

The Department in charge of Procurement shall take the necessary measures in order to implement this Policy especially through the appropriate provisions to be included in the Agency's procurement tenders, contracts, purchase orders and contracts performed by the Agency for third parties.

7.9 The service in charge of Corporate Compliance

The service in charge of Corporate Compliance shall conduct and monitor the implementation of this Policy, without prejudice to the duties and independence of the Data Protection Officer.

7.10 Agency's Staff Members

Each Staff Member has, in the framework of his/her functions, a general duty of:

i. *Care and protection of Personal Data*. Each Staff Members shall contribute to the implementation of the principles set forth in this Policy and in particular shall:
   a. treat any Personal Data with outmost care;
   b. refrain from any Processing of Personal Data that is not necessary, legitimate and appropriate in the light of his/her professional duties, of this Policy and of its implementing procedures;
   c. involve the Data Protection Officer, in a timely manner, as required by this Policy or the related procedures and guidelines; and,
   d. whenever it is involved in a Personal Data Processing, perform, as per modalities recommended by the Personal Data Officer, Personal Data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of the related risks (if any).

ii. *Cooperation.* Each Staff Member shall cooperate at all time with the Data Protection Officer, the Supervisory Authority and the Data Protection Committee in their area of responsibility.

iii. *Risk prevention and risk mitigation.* Each Staff Member shall identify at his/her level, the risks surrounding Personal Data protection and promptly inform his/her line management and the Data Protection Officer of any circumstances which may result in risks for the Personal Data protection.

7.11 Central Staff Association Committee (CSAC)

The CSAC may provide to the Director General input or recommendation when and to the extent Staff Members as Data Subjects are concerned in the following areas:

a. measures for the proper and effective implementation of this Policy within the Agency; and,

b. amendments to this Policy.

8. TRANSITION PERIOD

The first year after 1 March 2018 is a transition period, renewable upon decision of the Director General, during which:

(i) the Agency shall create the necessary procedures, guidelines and, generally ensure effective protection of Personal Data;

(ii) the Agency shall raise awareness and organise trainings related to the present Policy;

(iii) the Data Protection Officer shall perform regular consultations with the main organisational entities of the Agency which are directly concerned by Personal Data protection matters; and,

(iv) ongoing Personal Data Processing, implemented before the entry into force of the present Policy, shall be notified to the Data Protection Officer, who may make any recommendation considered appropriate in order to enhance the protection of Data Subjects. Such Personal Data Processing shall be brought into conformity with this Policy within the transition period.

9. ENTRY INTO FORCE –VALIDITY

This Policy enters into force on 1 March 2018, subject to its publication, without prejudice to the transition period set forth in Section 8 above. This Policy and its Annex may be amended as necessary, but it should be reviewed at the latest four years after its entry into force, to establish whether they require any amendment. Any amendment shall be issued upon decision of the Director General.

10. PUBLICITY

The present Policy is releasable to the public.

The Director General

ANNEX

GOVERNANCE SCHEME OF THE AGENCY'S PERSONAL DATA PROTECTION

The present Annex which forms an integral part of this Policy establishes pursuant to the ESA's Council Resolution on a "Personal Data Protection Policy", the detailed Personal Data Protection governance of the Agency which is based on the roles and responsibilities of:

I. The Data Protection Officer;

II. The Data Protection Supervisory Authority, served by a Registrar; and

III. The Data Protection Committee.

The implementation of this Policy and of the underlying procedures involve also other stakeholders as identified in this Policy and, more particularly, the ones referred to under its Section 7.

I Data Protection Officer

The Data Protection Officer and his/her deputy shall be Agency's Staff Members.

The deputy Data Protection Officer shall perform, on exceptional basis and under the same conditions as the Data Protection Officer, the same duties as those of the Data Protection Officer when the latter should be prevented.

Appointment

The Data Protection Officer shall be appointed by the Director General on the basis of professional qualifications in particular expert knowledge of Personal Data protection law and practices and may only be relieved of his/her position of Data Protection Officer by decision of the Director General.

In his/her capacity as Data Protection Officer, the Data Protection Officer has direct access to the Director General, keeping the service in charge of Corporate Compliance informed.

The contact details of the Data Protection Officer and his/her deputy will be published by means of an Information Note established by the service in charge of Corporate Compliance.

Duties

The Data Protection Officer and his/her deputy shall :

i. act as first point of contact concerning Personal Data matters;

ii. keep and update Personal Data Records, monitor the observance of this Policy and put in place controls and audits;

iii. examine any matter relating to Personal Data Protection and provide expert opinion in this field (e.g. impact assessments, risk mitigation plans, etc.), without prejudice to the competence of the Supervisory Authority;

iv. make recommendations to the Director General for :

   a. the effective implementation and monitoring of this Policy and for audit plans;

   b. the amendment of this Policy;

   c. the recognition of the Adequate Level of Protection or for the suspension or cancellation of recognition of the Adequate Level of Protection; or

d. any other matter related to the protection of Personal Data.

e. report on his/her activities to the Director General, after consultation with the the service in charge of Corporate Compliance;

v. initiate and deliver Personal Data protection training and generally contribute to Data Protection awareness activities for Agency's Staff Members, in cooperation with the Department in charge of personnel matters;

vi. following impact assessments to be performed by the relevant organisational entity of the Agency, authorise the Disclosure of Personal Data in the case mentioned in Section 5.3.2 iii. f. above; and,

vii. perform any other duties assigned to him/her by this Policy or by decision of the Director General.

Confidentiality

In the discharge of his/her duties, the Data Protection Officer (and his/her deputy) are bound to an obligation of confidentiality. Such obligation shall continue indefinitely after the termination of their appointment as Data Protection Officer.

Independence

In the discharge of his/her duties as Data Protection Officer, the Data Protection Officer (and his/her deputy) shall act independently and not be subjected to instructions from their hierarchy save that of the Director General provided such instructions do not constitute or amount to constitute a breach of this Policy and that of the principles adopted by Council in its Resolution on "Personal Data Protection Policy".

Consultation

In the performance of his/her duties, the Data Protection Officer (and his/her deputy) may seek for the opinion of, or input from, any organisational stakeholder of the Agency and, via the applicable communication channel, from the Central Staff Association Committee (CSAC).

For the responsibilities set forth in Section I iv. d) he/she may also seek for the opinion of the Data Protection Committee.

For the responsibilities set forth in Section I iv. a), b) and c) he/she shall seek for the opinion of the Data Protection Committee, without prejudice to the duties and independence of the Data Protection Officer.

II Data Protection Supervisory Authority (Supervisory Authority)

An independent Supervisory Authority has been established by Council in order to examine Incidents following decisions of the Agency in the field of Personal Data Protection, upon a complaint lodged by a Data Subject in accordance with Section 5.4.1 iv. of this Policy.

The Supervisory Authority shall be solely and directly accountable towards the Council for carrying out its functions in accordance with this Policy.

The members of the Supervisory Authority (including alternate members) shall perform their responsibilities in accordance with this Policy.

Composition and appointment

The Supervisory Authority shall consist of three members and one alternate member with proven expertise and experience in the field of Personal Data Protection.

The alternate member shall perform the same responsibilities as the members of the Supervisory Authority, if the latter should be prevented.

The members and the alternate member shall not be Staff Members or members of delegations of Members States, Associate Member States or Cooperating States.

The Supervisory Authority shall elect among its a Chairman and a Deputy Chairman.

The members and the alternate members of the Supervisory Authority shall be nominated by the Council for a three-years term, renewable for maximum three consecutive terms.

Confidentiality

In the discharge of their duties the members of the Supervisory Authority (and the alternate member) are bound to an obligation of confidentiality in accordance with their Rules of Procedure. Such obligation to continue indefinitely after the termination of their appointment by ESA Council.

Independence

In the discharge of their duties the members of the Supervisory Authority (and the alternate member) are independent. They shall neither seek nor take instructions from anybody.

Conflict of Interest

They shall not take part in a case in which they have a conflict of interest, notably if:

- they have a personal interest in the case;
- they have been previously involved as representative of one of the parties; or
- they participated in preparing the decision challenged.

In such case, either party may ask for a change in the composition of the Supervisory Authority.

Rules of Procedure

The Director General establishes the Rules of Procedure for the Supervisory Authority, which shall be approved by the Council.

Such Rules of Procedure for the Supervisory Authority are the ones adopted by ESA Council under Annex II of its Resolution on a Personal Data Protection Policy.

Decisions

The decisions of the Supervisory Authority are final and shall be binding to all involved parties.

Privileges and Immunities

As external experts, the members of the Supervisory Authority (and alternate members) shall enjoy the privileges and immunities provided for in Article XVII of Annex I to the ESA Convention.

Expenses

Only mission expenses incurred by the members of the Supervisory Authority in the performance of their duties shall be reimbursed by the Agency and this in accordance with the rules applicable to experts.

Facilities and Seat

The Agency shall provide for all necessary facilities in order to ensure the functioning of the Supervisory Authority.

The Supervisory Authority shall have its official seat at the Headquarters of the Agency; it may meet at other places if necessary.

Registrar. Procedure

The Council shall appoint a Staff Member to serve as Registrar of the Supervisory Authority.

The Registrar is responsible for matters of current administration of the Supervisory Authority and for all communications and discharge his duties in accordance with the Rules of Procedure set under Annex II of the Council's its Resolution on a Personal Data Protection Policy.

In the discharge of his duties, he/she shall be subject to the instructions of the Supervisory Authority.
In the discharge of his/her duties the Registrar shall not be subjected to instructions from his/her hierarchy.

The Registrar shall be afforded the necessary time to perform such duties.

In the discharge of his/her duties the Registrar is bound to an obligation of confidentiality. Such obligation to continue indefinitely after the termination of his/her appointment by ESA Council.

III. Data Protection Committee

The Director General establishes a Data Protection Committee which shall discharge its duties in accordance with this Policy.

Composition
The Data Protection Committee is composed by:

a. the representative of the service in charge of Corporate Compliance who chairs the Committee;

b. as relevant, by:
   i. the ESA Records Manager;

   ii. one Agency's Staff Member from each of the following Departments/Services, appointed for this purpose by the Heads of the Departments/Services:
   - Legal affairs,
   - Personnel matters,
   - Procurement,
   – ESA Security Office,
   - Corporate Information Technology; and

   iii. one member appointed by the Chair of the Central Staff Association Committee.

The above members shall attend and act within their area of responsibility.

Meetings
The Data Protection Committee is convened by its Chair.

Duties
The Data Protection Committee shall, upon request of the Data Protection Officer, provide its input, opinions or recommendations decided in application of the Section I above.

Confidentiality Duties
In the discharge of their duties the Chair and the members of the Data Protection Committee are bound to an obligation of confidentiality. Such obligation shall continue indefinitely after the termination of their membership.