

# **IEA PRIVACY MANAGEMENT PROGRAMME**

Effective Date: 4 October, 2023

## IEA PRIVACY MANAGEMENT PROGRAMME

Pursuant to Art. 10(b) of the *Decision of the Secretary-General on the Protection of Individuals with regard to the Processing of their Personal Data* ("the **Data Protection Rules**"), the OECD Secretary General adopted guidelines in order to establish a [Privacy Management Programme for the OECD](#). The OECD Privacy Management Programme follows the [OECD Privacy Guidelines](#) (Part Three).

The International Energy Agency (IEA), an autonomous agency within the framework of the OECD, is also subject to the Data Protection Rules and its Executive Director is responsible for ensuring that processing of personal data at the IEA complies with the Data Protection Rules. In accordance with the abovementioned guidelines and in consultation with the IEA, the Data Protection Officer has established this Privacy Management Programme (**PMP**) for the IEA which reflects the IEA's specific governance and operations. Where this PMP uses terms that are defined in the Data Protection Rules, those terms shall have the same meaning as in such rules.

### Scope of this IEA Privacy Management Programme

1. This PMP for the IEA helps the IEA meet the accountability requirements in the Data Protection Rules [Art. 6 Data Protection Rules].

### Roles and responsibilities

2. The Data Protection Rules articulate clear roles and responsibilities for the controller and processors, including those working at the IEA,<sup>1</sup> as well as the Data Protection Officer, Data Protection Commissioner, and the OECD Secretary-General. The active engagement of a number of other actors across both the OECD and the IEA is also required to support the data protection function. This engagement is additional to responsibilities these actors may have as controller or processors for activities under their responsibility. In consultation with the Data Protection Officer and Data Protection Commissioner where appropriate, the following actors at the IEA support the IEA's data protection function:

- **Executive Office (EXO)** – provides leadership to the IEA regarding the importance of data protection and support to the operations of the Data Protection Officer and Data Protection Commissioner, including through the provision of necessary resources and administrative support. Furthermore, the IEA Executive Director has delegated to the IEA's Chief Information Security Officer (**CISO**) overall decisional authority for the implementation of information security measures (including those to protect personal data) and actions regarding security incidents (including personal data breaches), as may be approved by the IEA's Information Security Board.

---

<sup>1</sup> Including when the Organisation itself acts as a processor.

- **Information Security Board (ISB)** – approves and oversees the IEA’s implementation of technical and organisational measures to implement the Data Protection Rules, to ensure that processing is carried out in accordance with the Data Protection Rules and to protect against personal data breaches. The ISB also supports IEA-wide communications in such respect.
- **ISB Working Group (ISB WG)** – proposes technical and organisational measures to implement the Data Protection Rules, ensure that processing is carried out, and continues to be carried out, in accordance with the Data Protection Rules, deal with and protect against personal data breaches, and to achieve continuous improvement of personal data protection at the IEA. This includes integrating data protection considerations in the information security policy development process. The ISB WG also recommends incident response policy and guidance that includes protocols to support an IEA controller in meeting their data breach notification obligations [Art. 6.4 Data Protection Rules] and reviews personal data breaches.
- **Information Security Officer** – a position held by the **Head of the Information Systems Unit (ISU)** within the **IEA’s Office of Management and Administration (OMA)** – provides technical advice to the CISO and ISB WG on the appropriate security measures for processing personal data.
- **IEA Office of the Legal Counsel (OLC)** – provides advice to the IEA and inputs to the ISB WG on legal aspects related to the interpretation and implementation of the Data Protection Rules, in particular in data sharing arrangements and agreements with third parties. Additionally, in coordination with the OECD’s Programme of Budget and Finance’s Corporate Procurement Group and the OECD’s Directorate for Legal Affairs, OLC helps ensure that data protection risks and requirements are addressed during the procurement and contracting process.

### **Internal co-ordination**

3. The integration of the data protection function across regular IEA business activity is critical for maximising impact and leveraging resources.
  - a) The Data Protection Officer should be invited to engage and participate in relevant co-ordination groups at the IEA, such as those addressing IT co-ordination, digital strategies, digital and information security, and data governance.
  - b) The Data Protection Officer may occasionally interact with the Group of Directors, including the IEA Executive Director, and communities and networks for Organisation-wide resource management advisors, counsellors, and communications and IT specialists in which personnel representing the IEA take part.

### **Policy integration and coherence**

4. The Data Protection Rules operate within the broad framework of rules and regulations

governing the Organisation, including those applicable to the IEA, and shall be applied with reference to that framework. In particular, the Data Protection Rules should be applied in a manner that gives effect to the following Staff Regulations:

- a) Officials shall not be subject to discrimination on the grounds of racial or ethnic origin, nationality, opinions or beliefs, gender, sexual orientation, health or disabilities [Staff Regulation 5(a)].
- b) Officials are entitled to respect for their privacy [Staff Regulation 5(c)].

### **Data protection risk assessment**

5. The IEA should implement the OECD's risk-based approach to data protection as is reflected in the Data Protection Rules.

- a) The Data Protection Officer should maintain a methodology to assist the IEA controller in conducting a Data Protection Risk Assessment and identifying appropriate safeguards to mitigate the risks [Art.6.2 Data Protection Rules].
- b) A single assessment can be carried out for multiple or repeated activities at the IEA that pose similar risks, such as organising IEA events and meetings and operating the IEA website.

### **Personal data inventory**

6. Strong record-keeping practices are a foundation for data protection compliance and facilitate the IEA's capacity to prioritise and manage risks, respond to individual rights requests and to facilitate transparency.

- a) Building on the record-keeping required of the controller and processors [Art. 6.1(b) Data Protection Rules] as well as the consultations on data protection risk assessment [Art. 6.2 Data Protection Rules], the Data Protection Officer, in liaison with the IEA's DP and IT Focal Point (see paragraph 8(b) below), should develop and maintain an inventory of personal data processing activities at the IEA.
- b) The development and maintenance of the IEA's personal data inventory should be coordinated with other inventory initiatives linked to sensitive data, statistics and data, and IT systems and infrastructure.

### **Procurement and contracts**

7. To ensure that the IEA's processors meet their responsibilities under the Data Protection Rules [Art. 6 Data Protection Rules] and consistent with the principle of Data Protection by Design [Art. 6.3 Data Protection Rules] the IEA should implement data protection measures as part of its procurement process.

- a) When the OECD procures services on the IEA's behalf that involve the processing of

personal data, the market consultation or call for tender should inform candidates that they must demonstrate their capacity and willingness to provide contractual guarantees consistent with the requirements for data processors under the Data Protection Rules and comply with any applicable data protection regulations.

- b) In general, data protection (and related digital security) capabilities should be treated as minimum requirements as part of the procurement process.
- c) The IEA should use the OECD's model data protection clauses in contracts that involve the processing of personal data, including contracts for which no competitive procurement process is required. These should include a default set of basic protections with stronger measures available for inclusion as appropriate to the context and risks.

### **Training, education, and awareness**

8. Effective implementation of data protection measures requires that all staff and other personnel working at the IEA involved with the processing of personal data have a basic awareness about when the Data Protection Rules apply, what compliance entails, and when to seek the advice of the Data Protection Officer.

- a) The Data Protection Officer should develop training and educational materials, such as eLearning courses and "How-To" guides, to aid staff in understanding their data protection responsibilities. The ISB WG and/or the IEA DP and IT Focal Point may also develop similar materials that are specifically tailored for the IEA. These materials should be available on the OECD and IEA Intranets, as appropriate and promoted through regular communications channels. Relevant information should be provided to new staff as part of the onboarding process.
- b) The IEA should maintain a focal point to represent the IEA within the OECD's network of focal points who will work with the Data Protection Officer, the Digital Security Office, the ISB and the ISB WG to facilitate communications, identify privacy and security issues raised by the IEA's day-to-day work, and embed good practices as part of the IEA's workplace culture (the "**IEA DP and IT Focal Point**").
- c) The IEA should undertake occasional awareness-raising activities.

### **Transparency and external visibility**

9. As an accountable organisation, the IEA should be transparent about its commitment to data protection, the rules it follows and the practices put in place, as well as providing specific information about activities involving the processing of personal data.

- a) The IEA should make public its approach to data protection, posting links on its website to this PMP, and the Data Protection Rules available on the OECD's website.

- b) The IEA should follow a layered approach to transparency regarding the personal data it processes, in particular for data subjects who are not staff members. A general description of its approach to data protection and types of data processing activities should be available on the IEA website, with links to general notices for regular processing activities (e.g., website visitors, event participants and visitors to the IEA premises). For projects involving larger scale data processing, a data protection notice should be available on the project pages on the websites. In addition, specific notices should be made available directly to data subjects as necessary.

### **Data subject rights**

10. Data subject rights requests [Art. 5 Data Protection Rules] should be responded to without undue delay, and generally within one month.

- a) The collection of additional data to verify the identity of the requestor should be minimised as far as possible, consistent with the need to authenticate the request and consequences of a possible error.
- b) The controller should ensure that responses to a request are reviewed to prevent adverse effects on other data subjects and that any personal data transmitted in response to a request is protected with appropriate security measures.

### **Monitoring and review**

11. While remaining consistent with the Data Protection Rules, this PMP should be reviewed and adapted to reflect changes in the IEA and OECD practices regarding the processing of personal data and the evolution of the IEA's data protection and information governance maturity.

- a) The PMP review process should be conducted every two years and be led by the ISB WG in consultation with the IEA DP and IT Focal Point and the Data Protection Officer.
- b) In addition to updates or changes that may be needed to existing sections, consideration is given to including additional elements in the future, for example to improve monitoring and metrics.