SECRETARY-GENERAL'S GUIDELINES ESTABLISHING THE OECD PRIVACY MANAGEMENT PROGRAMME

Effective Date: 28 October 2022

SECRETARY-GENERAL'S GUIDELINES ESTABLISHING THE OECD PRIVACY MANAGEMENT PROGRAMME

These Guidelines are adopted 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") and shall be read consistently with the Data Protection Rules. Where these Guidelines use terms that are defined in the Data Protection Rules, those terms shall have the same meaning as in these Rules.

Adaptation of these Guidelines may be required to reflect the specific governance and operations of entities and bodies within the OECD framework, such as the International Energy Agency (IEA), OECD Nuclear Energy Agency (NEA), and the International Transport Forum (ITF). Such adaptations should be established by the Data Protection Officer, following consultation with the entity or body affected.

Scope of these Guidelines

1. Following the OECD Privacy Guidelines (Part Three), this document establishes a Privacy Management Programme (PMP) to help the 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,[1] as well as the Data Protection Officer, Data Protection Commissioner, and Secretary-General. The active engagement of a number of other actors across the Organisation 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.

- **Office of the Secretary General (OSG)** – provides leadership to the Organisation 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.

- **Executive Directorate (EXD)** – supports the integration of data protection considerations in the IT policy development process and in Organisation-wide communications.

- **Digital Security Office (EXD/DKI/DSO)** – provides advice on the appropriate security measures for processing personal data and establishes incident response policy and guidance that includes protocols to support the controller in meeting data breach notification obligations [Art. 6.4 Data Protection Rules].

- **Directorate for Legal Affairs (SGE/LEG)** – provides advice to the Organisation on legal aspects related to the interpretation of the Data Protection Rules, in particular in data sharing arrangements and agreements with third parties.

- **Programme of Budget and Finance (EXD/PBF)** – helps ensure that data protection risks and requirements are addressed during the procurement and contracting process, in co-ordination with SGE/LEG.

[1] Including when the Organisation itself acts as a processor.

- **Directorate for Public Affairs and Communication (PAC)** – helps raise awareness of data protection issues in the context of its work to co-ordinate communications and stakeholder interactions for the OECD.

- **Directorate for Statistics and Data (SDD)** – helps raise awareness of data protection issues as part of its co-ordination of the work of the statistics and data community and in the context of data sourcing and management strategies.

Internal co-ordination

3. The integration of the data protection function across regular business activity is critical for maximising impact and leveraging resources.

a) The Data Protection Officer should regularly engage and participate in relevant co-ordination groups across the Organisation, such as those addressing IT co-ordination, digital strategies, digital and information security, and statistics and data governance.

b) The Data Protection Officer may occasionally interact with the Group of Directors, and communities and networks for resource management advisors, counsellors, and communications and IT specialists.

Policy integration and coherence

4. The Data Protection Rules operate within the broad framework of rules and regulations governing the Organisation 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 Organisation should implement a 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 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 that pose similar risks, such as organising events and meetings.

Personal data inventory

6. Strong record keeping practices are a foundation for data protection compliance, and facilitate the Organisation'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 should develop and maintain an inventory of personal data processing activities.

b) The development and maintenance of the personal data inventory should be co-ordinated with other inventory initiatives linked to sensitive data, statistics and data, and IT systems and infrastructure.

Procurement and contracts

7. In order to ensure that the Organisation'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 Organisation should implement data protection measures as part of its procurement process.

a) When the Organisation procures services 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 capabilities should be treated as minimum requirements as part of the procurement process.

c) The Organisation should maintain model data protection clauses to be included 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 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. These materials should be available on the Intranet and promoted through regular communications channels. Relevant information should be provided to new staff as part of the onboarding process.

b) The OECD should maintain a network of focal points designated by each directorate/service to work with the Data Protection Officer and the Digital Security Office to facilitate communications, identify privacy and security issues raised by day-to-day work, and embed good practices as part of the Organisation's workplace culture.

c) The Organisation should undertake occasional awareness-raising activities, such as annual communications on International Data Protection Day.

Transparency and external visibility

9. As an accountable organisation, the OECD 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 OECD should make public its approach to data protection with links to the Data Protection Rules, this PMP, and the Data Protection Commissioner's Annual Activity Reports.

b) The OECD 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 OECD website, with links to general notices for regular processing activities (e.g., recruitment, website visitors, visitors to the 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 OECD practices regarding the processing of personal data and the evolution of the OECD's data protection and information governance maturity.

a) The PMP review process should be conducted every two years, and be led by the Data Protection Officer in consultation with the Data Protection Commissioner, as well as the Office of the Secretary-General and Office of the Executive Director. Consultation may also include others identified in paragraph 2 above.

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.