OECD

ANNUAL ACTIVITY REPORT OF THE DATA PROTECTION COMMISSIONER

2019

Billy Hawkes
January 2020

Table of Contents

Introduction

This is my first report as Data Protection Commissioner (DPC), following my appointment by the Secretary-General on 3rd May 2019. It reports on implementation by the OECD of the revised data protection rules put in place at the same time, summarises the main areas where I have intervened over the first months of implementation, my actions in terms of awareness raising and the number of claims treated and their overall results. It also looks forward to plans for further strengthening of the regime in 2020.

Revised Data Protection Rules

The OECD was a pioneer in developing internationally accepted privacy and data protection principles. The OECD Privacy Guidelines have served as the basis of many national and regional data protection regimes. They remain highly relevant and form the basis of the new internal OECD regime.

As an independent intergovernmental organisation, the OECD is not subject to national or regional legislation. With respect to data protection, the OECD is governed by its own internal rules, currently set out in the "Decision of the Secretary-General on the Protection of Individuals with regard to the Processing of their Personal Data" (the "Decision" or "Rules"). The Decision entered into effect on 3 May 2019 and elaborates how the principles in the OECD Privacy Guidelines are to be given practical effect within the OECD. It also reflects recent developments in the data protection legislative environment. It further builds on the experience gained through the operation of the previous internal OECD data protection regime which it replaced and aligns the personal data protection provisions at the OECD with best standards.

Main Features of Rules

The Rules provide a comprehensive framework governing the processing of personal data by or on behalf of the OECD. The main categories of such data are those of OECD staff, of delegates and visitors to the Organisation and of individuals included in OECD projects.

Accountability is a key principle underlying the Rules, with "Coordinators" – in practice, Directors and Agency heads – being held accountable for the proper stewardship of personal data in their directorates/agencies. The rules include a number of key features, including processing principles, individual rights, and implementation and oversight mechanisms.

Principles related to Processing

The Decision applies to the processing of all personal data by or on behalf of the Organisation, requiring that personal data be:

- processed in a transparent manner and for specified, explicit and legitimate purposes for the delivery of the Organisation's mission and programme of work;
- adequate, relevant, accurate, reasonably kept up to date, and limited to what is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures their appropriate security, using appropriate technical or organisational measures to the extent reasonably possible; and
- kept for no longer than is necessary for the purposes for which the personal data are processed.

The Decision imposes significant limitations related to the processing of sensitive personal data as well as for automated processing, including profiling. Likewise, high risk processing is subject to specific protections.

Rights of Individuals

The Decision also provides rights for individuals with respect to their personal data, which individuals can assert directly with the Coordinator.

Individual Rights

Transparency and information

- Information on processing available on the intranet and/or internet websites of the Organisation
- Information on processing available to specific individuals, on their request

Right of access

- Allowing individuals to know if their personal data are processed and to access such personal data

Right to rectification and erasure

- Allowing individuals to request rectification or completion of inaccurate personal data
- Allowing individuals to request erasure of personal data

Right to object

- Allowing individuals to object when processing is not necessary for the OECD mission

Right to data portability

- Allowing individuals to get and re-use their data for different services

Implementation Framework

Responsibility for compliance and putting in place appropriate technical and organisational measures is with Coordinators. The creation or renewal of a data processing activity triggers the need for prior consultation with the Data Protection Officer (DPO). Risk Assessment is mandatory, with data protection by design and default integrated into the process to ensure that data protection and privacy issues are considered upfront.

Appropriate technical and organisational measures must be taken to ensure a level of security reasonably appropriate to the risk. Personal data breaches have to be reported to the Data Protection Commissioner (DPC) and DPO within 48 hours and to concerned individuals without undue delay.

Appointment of DPO and DPC

The Decision created two new roles at the OECD: the Data Protection Officer and Data Protection Commissioner, both to support the implementation of the Rules by OECD. Following an initial

period in an interim capacity, the Secretary-General appointed Michael Donohue to the DPO role after an open competition. I was appointed as DPC for a five-year term. The DPO role involves support for day-to-day implementation of the Rules while that of the DPC is largely one of external oversight, including necessary enforcement. The details of the roles, as set out in the Decision, are summarised below.

Data Protection Officer

Mandate

- expert with knowledge of data protection regulations, policies and practices
- appointed as an OECD official and reports directly to the Secretary-General
- performs duties in a fully neutral manner and in full independence

Responsibilities

- provide information and advice regarding Decision to OECD staff and contractors
- promote awareness and provide for training of staff
- provide information and advice to individuals regarding the processing of their personal data and the exercise of their rights under the Decision
- take measures to ensure compliance with the Decision
- verify any processing
- decide on the temporary suspension for high risk processing
- provide information and assistance to the DPC

Data Protection Commissioner

Mandate

- ensure and enforce the Decision
- performs mandate independently and in a fully neutral manner
- appointed by Secretary-General for a fixed term of 5 years

Responsibilities

- assist and advise on data protection risk and its treatment
- investigate claims alleging breach of rules
- notify Coordinators of infringements

Investigative and Corrective powers

- communicate a personal data breach to the individuals concerned
- rectify or erase personal data or restrict processing
- suspend, limit, or ban a processing
- communicate to the Secretary-General general comments aimed at ensuring the protection of personal data
- submit an annual activity report to the Secretary-General

Activities 2019

Introduction

In the seven months since the Rules came into effect, the focus has been on building on the existing strong privacy framework within OECD. Particular effort has been devoted to communicating to internal and external stakeholders the more demanding requirements set out in the Rules and having these requirements integrated into standard operating procedures and protocols. This has involved close co-operation with the Executive Directorate, particularly the recently strengthened Digital Security Office, and the Directorate for Legal Affairs. Ensuring the continued safe transfer of data between OECD and its Members has also been a significant focus.

Data Mapping

An important step in building and managing a data protection programme is to create an inventory of all the personal data processing activities across the Organisation. This is necessary both for ensuring

that the appropriate protections are in place and to enable appropriate responses to requests by individual to assert their rights.

One tool developed to assist in the mapping process is the Personal Data Protection Processing Form, which is available on the Intranet. The form assists Coordinators in meeting their responsibilities for information provision, prior consultation, and risk assessment. For projects that involve new IT requests, questions from the data protection form have been integrated into a broader request form covering IT needs and security issues in a co-ordinated manner.

Preliminary results from mapping activity to date indicate that the OECD processes personal data in support of its mission for purposes that can be bundled into three broad categories:

1. To manage and provide benefits to staff and as part of its recruitment process.
2. To facilitate participation by delegates and other individuals in official meetings, events, projects, and to enable access to OECD websites, communications and publications.
3. To produce evidence to support the policy making process

The type of human resources processing in the first category is commonplace across many organisations of similar size to the OECD. The data processed as part of the OECD's role as hub for government officials and experts largely involves the processing of professional contact details and details of their interactions with the OECD.

The data processing in the third category can be more complex. For some projects, personal data is obtained directly from individuals (e.g. Compare your Income) or via a service provider to the OECD (e.g. Risks that matter). Other projects in the third group involve personal data collected by OECD members and then transferred to the OECD or its contractor. In these cases, the members will be subject to their own national data protection laws, and typically only de-identified data is transferred. Examples of such projects include:

Examples of projects involving personal data obtained from governments or third parties

- *Programme for International Student Assessment* (PISA) (survey of 15-year-olds' ability to use their reading, mathematics and science knowledge and skills)
- *Programme for the International Assessment of Adult Competencies* (PIAAC) (survey of adult's proficiency in key information-processing skills)
- *Teaching and Learning International Survey* (TALIS) (survey of teachers and school leaders about working conditions and learning environments)
- *Study on Social and Emotional Skills* (survey of 10- and 15-year-old students that assesses the conditions and practices that impact the development of social and emotional skills)
- *International Early Learning and Child Well-being Study* (IELS) (survey that assesses children at age 5 across 3 countries, identifying key factors on the development of early learning)
- *Patient-Reported Indicators Survey* (PaRIS) (survey of experiences for patients with chronic conditions who are treated in primary health care or other ambulatory health care settings)
- *Data on enforcement and monitoring of the Anti-Bribery Convention* (data on criminal, administrative and civil cases for offences related to foreign bribery)

Considerable work remains to be done to fully map the Organisation's data holdings, and the resulting inventory will need to be regularly updated as projects are completed and new ones started. The mapping exercise has links to related efforts underway in the Digital Security Office, as well as a survey

conducted by the Statistics and Data Directorate of the OECD's projects involving statistics and data outputs.

Information/Awareness

Transparency is a core element of data protection and privacy, and the Decision includes a number of related requirements.

Intranet/Internet

Publishing the Decision on the OECD's Intranet and Internet sites was a prerequisite to the Decision entry into force in May. A new internal page was created for the Intranet to describe the Decision and link to it. Likewise the OECD's privacy policy page was updated in May to reflect the new Decision.

Later, a new overview page was created for the public site to provide general information about the OECD's internal approach to data protection in the context of its activities. Following a "layered" approach to the provision of information to individuals, specific notices are being prepared for different activities, with the overview page serving as a hub. The privacy policy addresses data collection in the context of visitors to the OECD website. There is a specific notice focused on recruitment that was updated to reflect the Decision.

Further work to improve information provision through data protection notices is underway. The DPO has prepared a data protection notice template that can serve as a starting point for staff and helps ensure that all required elements are included. One example is a notice being prepared for data processing associated with delegates and other visitors to the OECD. Work is also underway across the entities and bodies within the OECD framework (such as IEA, NEA, ITF) to update their website privacy policies to reflect the Decision. These efforts have been facilitated by the preparation of a template privacy policy to bring some consistency and simplicity to the notices being updated.

Efforts are also underway to develop project-specific notices where appropriate. For example, the development of a new mobile app for use by conference attendees has also generated a need for its own notice. Conference-specific sites are being updated to include additional information where the event will involve data processing activity that goes beyond that described in the more general notices (e.g. that an event will be webcast).

"How to" Guides for Staff

The DPO has prepared a set of "How to" guides for staff providing advice on compliance with the Decision in the context of several regular activities. These guides are posted in the "How to" section of the Intranet site and promoted through communications channels such as the "Tip of the Week" and "EXD Essentials".

Data Protection "How To" Guides

- How to handle an individual rights request
- How to prepare data protection notice
- How to handle participants lists

As we gain greater implementation experience, additional topics will be identified as subjects for these practically-orientated communication tools with a view to raising awareness and promoting good practice.

Internal Engagement and Visibility

Integrating data protection into the day-to-day operations of the Organisation is the best strategy for raising awareness and achieving compliance. To this end, having staff meet and engage with the DPC and DPO has been a priority in these first months under the Rules. During 2019 I made several visits[1] to the OECD, meeting with the Secretary-General, Chief of Staff, and the EXD and LEG leadership, as well as staff in substantive directorates. I also participated with the DPO in a meeting of the Group of Directors chaired by the Secretary-General, which included an agenda item devoted to the Rules. This provided an important opportunity to highlight to Directors their vital role and responsibilities under the Decision.

With my support, the DPO is now a regular member or participant in a number of co-ordination groups across the Organisation. These include:

- Information Technology Coordination Group (ITCG)
- Information Security Governance Group (ISGG)
- Statistics and Data Board at Manager's level (SDB-M)
- Statistics and Data Community of Practice on Microdata
- Correspondant Informatique (CI)

He has also been in contact with the network of Resource Management Advisors (RMAs), Counsellors network, and Senior Communications Board to establish a regular dialogue with colleagues particularly well positioned to identify data protection issues as they arise.

A joint awareness raising activity with the Digital Security Office is being planned on 28 January 2020, to mark International Data Protection Day. It is expected to include messaging to all staff, the launch of several "How to" guides, and two panel discussions focussed on how strong data governance can facilitate access to the data sources needed for policymaking. I will participate in the discussions and hope to engage staff in the issues, highlighting that good privacy and security are not only essential to protect individuals but also serve as an enabler for advancing the Organisation's public interest mission.

External Engagement and Visibility

The Rules are intended first and foremost to improve the Organisation's ability to protect individuals in the context of its data processing activities. The Rules also enable the Organisation to match its

[1] Dates: 16 April; 20-21 May; 17-18 June; 9 July; 29 October.

internal practice to its long-standing public policy leadership in this area. Moreover, obtaining the data needed to conduct its policy analysis is increasingly reliant on the credibility of the Organisation's ability to provide the privacy and security protections demanded by outside data sources. As a result, external engagement and visibility is also an important ingredient of implementation success.

External outreach efforts in 2019 included engagement with the community of data protection officials in other international organisations as well as the broader data protection community. Shortly after the Rules took effect, the DPO and I travelled to Brussels to introduce the Rules to European Commission officials and engage in dialogue on the international transfer issues discussed below.

On 17-18 June, the OECD co-hosted with the European Data Protection Supervisor the annual workshop on Data Protection in International Organisations. We welcomed 90 participants representing more than 40 different organisations to discuss the common challenges we face in implementing data protection across our activities.

In October, I was approved as a new member of the Global Privacy Assembly (formerly the International Conference of Data Protection and Privacy Commissioners) and participated in the 41st meeting in Tirana, Albania. I was joined by the DPO and other OECD colleagues participating as observers. The conference provided a useful opportunity for side meetings with the European Commission, and a number of data protection authorities.

Provision of Advice/Prior Consultation

The primary role of the DPO is to provide advice to staff on their responsibilities under the Rules, and I support him in that role through regular exchanges on particular issues. During 2019, the DPO was consulted regarding a large number of projects from across the Organisation and affiliated entities, covering a range of different data protection issues. The table below provides a sample of some of the subjects addressed in these consultations.

Selected Topics of DPO Consultations (2019)

meeting webcasts · translations · staff printing costs · office moves tool · green plates quiz · culture survey · CRM tool · staff training · service desk contract · access to staff accounts · student surveys · teacher surveys · events app · use of expert's data · surveys on religious tolerance · health microdata survey · email lists · staff surveys · participation lists · consultation survey · creation of observatory · use of staff CVs · stakeholder surveys · website privacy policy · video collection · income survey · conference registration · data transfers · contact lists · programme implementation reporting

Data Breaches

Two data breaches were reported following the entry into force of the Rules. One breach resulted from submission of a pension payslip to the wrong pensioner. The other breach resulted from the submission of tax-related data for five OECD pensioners to the wrong tax authority. Both incidents involved human error. Appropriate steps were taken in both cases to have the erroneous data deleted, notify the affected individuals and reduce the risks that these errors will occur again.

In addition, follow-up actions were taken in response to a personal data breach that occurred prior to the entry into effect of the Rules. The breach did not involve OECD systems, but rather the financial files of the OECD's medical claims provider. Some current and former OECD staff members were targeted by a fraudulent bank debit scheme as a result of the breach. Follow-up by the OECD DPO indicated that the provider had taken appropriate steps following the breach and co-operated with the OECD's own investigation of the matter.

Individual Rights Requests

A protocol for addressing individual rights requests has been established, and is reflected in a "How to" guide due to be published early in 2020. Three requests asserting individual rights under the Decision were received in 2019, each of which was complied with by the Organisation.

- The first was a request for erasure, which concluded with deletion of a recruitment profile created by the requester in the OECD's recruitment database.
- The second request was also for erasure and concluded with the deletion of the requester's "MyOECD" account.
- The final request concerned personal data contained in a presentation that the requester had submitted to the OECD to be made public. The presentation was promptly removed from the OECD website.

Claims and Use of Formal Powers

No individuals submitted a claim to me or the DPO in 2019.

No situations arose in 2019 requiring the use of my investigative or corrective powers under the Decision.

International Transfers under GDPR

An important issue for the Organisation has arisen with respect to transfers of personal data from EEA members required for participation in some OECD projects. These challenges arise due to the inclusion of international organisations in the restrictions on such transfers contained in the EU's General Data Protection Regulation (GDPR). The issue has come up, for example, in connection with the transfers required for important projects like PISA and PIAAC.

The challenges do not arise from questions about sufficiency of protections OECD puts in place for these programmes to address any risks to individuals. Nor do they relate to the strength of the data protection regime now in force at the OECD. Rather, the challenges concern the interpretation of certain requirements of the GDPR, which are not necessarily well-adapted to the legal status and international character of intergovernmental organisations like the OECD.

Although the OECD is not subject to GDPR our EEA members do have to comply. To help our EEA members, I have joined the DPO and the Legal Directorate in discussions with relevant EU authorities, including the European Commission and several national data protection authorities. I am pleased to report that there is both a recognition that the challenges need to be addressed and a willingness to find appropriate solutions to ensure that the data flows necessary for the important public interest work of the Organisation are not interrupted.

Looking forward to 2020

During the first seven months which I have served as DPC considerable progress has been made in putting in place the processes and practices necessary to establish a top class data protection programme at the OECD. There is still, however, much to be done to further mature the operations of the new regime.

Priorities for the data protection function in 2020 include:

- ***Data mapping***: A comprehensive mapping of personal data processing activities is essential to enable a proper risk assessment by Coordinators and the prioritisation of efforts to address those risks. Further work is needed to complete the inventory of the personal data uses across the Organisation and make the outcomes transparent. Particular attention should be directed to processing activities outsourced to third parties and the use of cloud applications. Continued co-ordination with parallel work by the Digital Security Office will be mutually beneficial.
- ***Data protection notices***: The introduction of the layered approach to notices in 2019 needs to be expanded across the full range of websites and activities underway in the OECD and other bodies under the OECD framework.
- ***Awareness-raising and training***: Building on the International Data Protection Day activities in January 2020, additional efforts will be needed to raise awareness about the Rules, with particular attention to highlighting the need for greater transparency around the processing of delegates and visitor data. A plan for introducing training activities will also be developed, ideally integrating data protection with digital security and co-ordinated with other OECD training programmes.
- ***Data breach incident response*:** All organisations need to be prepared to respond to a security incident that results in a breach of personal data. The OECD Rules have specific notification requirements, and guidance for staff should be developed, in co-operation with the Digital Security Office***.***
- ***International transfers***: Continued efforts will be needed to help EEA members address the GDPR challenges related to transfers of personal data to OECD.

These priorities are additional to the day-to-day work of providing advice to staff on compliance and good practice, and responding to any individual rights requests or complaints. Following the one-year anniversary of the Rules in May 2020, we may have gained sufficient experience for a first reflection on how the Rules are functioning and whether the resources and governance structures are appropriate to the task.