OECD

ANNUAL ACTIVITY REPORT OF THE DATA PROTECTION COMMISSIONER

2021

Billy Hawkes

January 2022

Table of Contents

Introduction

This is my third Annual Activity Report as Data Protection Commissioner (DPC), following my appointment by the Secretary-General in May 2019. The submission of this report is part of my responsibilities as enumerated in the *Decision of the Secretary-General on the Protection of Individuals with regard to the Processing of their Personal Data* (Data Protection Rules) [Article 8.2(e)] which applies to all personal data processed by or on behalf of the Organisation in fulfilment of its mission. A summary of the Data Protection Rules can be found in my 2019 Activity Report.

This report summarises the main developments in relation to the Data Protection Rules during 2021 including the initiatives taken by the Data Protection Officer (DPO) and the OECD more generally to ensure their effective implementation. As in my 2020 Activity Report, my conclusion looks forward to plans for continuing to strengthen the data protection function in the coming year.

As provided by the Data Protection Rules, this report will be made available to the public along with my previous reports on the main data protection page of the OECD website. This practice is also consistent with the longstanding focus on transparency and organisational accountability reflected in the OECD Privacy Guidelines.

Activities in 2021

Internal Engagement and Processes

The OECD has a long experience of respecting privacy and data protection in its own data processing activities (as distinct from its policy work in this area) with internal rules dating back more than twenty years. In that sense, the introduction of new rules in 2019 has not required significant overhaul of existing practices. In many areas the Organisation has simply reinforced existing good practice. In some areas, however, the Organisations has made important improvements and introduced new processes – in particular to adapt to a stronger set of individual rights and a new governance structure reflected in the roles of the DPO and DPC. My prior two annual reports documented a number of those improvements, to which I add below some areas that served as a particular focus in 2021.

Information/Awareness

The Data Protection Rules include a number of requirements related to transparency and awareness, areas which require ongoing attention. It is a specific responsibility of the DPO to promote awareness and provide training [Article 7.4(b)]. Following the practice established in 2020, the Secretary-General sent out an all-staff message on 28 January 2021, to mark the OECD's observance of International Data Protection Day. In addition to circulating my annual report, the message encouraged staff participation in a sensitive data inventory exercise and also encouraged staff to consult the growing library of educational materials on data protection and digital security. It further recalled the mutually reinforcing linkage between the Organisation's policy work and its commitments to good internal practice. New materials developed in 2021 included a "How To" guide on staff surveys, released in part to reflect the increasing use of such surveys to understand the impact of the COVID-19 measures on working life.

Launch of data protection eLearning course

With my encouragement and with the support of the Executive Directorate, the DPO helped design an eLearning course specifically tailored to the OECD's data protection regime and data processing activities. The course begins with a discussion of personal data and the common types of personal

data processed at the OECD. It then moves the learner through the key steps for complying with the Rules, highlighting key actors like the DPO and DPC, but also the important roles played by the Directorate for Legal Affairs and the Digital Security Office. The course then walks the learner through typical activities like conducting a staff survey, organising events and hiring a survey firm to conduct policy research. Interactive throughout, the course concludes with a quiz to help reinforce key concepts and test the learner's knowledge. Launched in November 2021, with an all-staff communication and as the "Tip of the Week", staff members have begun to take the course and many have provided useful feedback. Information about the course is now included in the on-boarding materials for new staff and will be the subject of additional communication campaigns in 2022.

Data Protection and Digital Security Focal Points

The OECD has begun a process to create a new network of Data Protection and Digital Security Focal Points. Recognising that organisational change is difficult, this initiative aims to embed privacy/security 'champions' across key business functions. Designated by each directorate/service, the focal points will work with the DPO and the Digital Security Office to improve communications channels, identify privacy and security issues raised by day-to-day work, and embed good practices as part of the Organisation's workplace culture. It will help enable the data protection and digital security functions to scale up to meet the governance challenges associated with the growing appetite for new data sources and uses at the OECD.

Data Mapping

The maintenance of an inventory of personal data processing activities across the Organisation is necessary to prioritise and manage risks, respond to individual rights requests and to facilitate transparency as required by Article 5.1(b). Efforts to map personal data across the Organisation continued in 2021 at a more granular level. A pilot was started to consider whether data protection record-keeping functionality can be integrated in a broader enterprise architecture solution for the Organisation. In addition to providing greater visibility and reporting capabilities regarding the processing of personal data, if adopted this sort of integration would help further embed data protection as part of the regular business of the Organisation.

Integration of the Data Protection Function

The integration of the data protection function across regular business activity is critical for maximising impact and leveraging resources. The DPO continues to serve as a member of the Organisation's community of Risk Focal Points, which helps ensure that data protection issues can be reflected in the biannual process to update the risk register in light of evolving risks. The DPO likewise regularly engages and participates in relevant co-ordination groups across the Organisation, such as those addressing IT co-ordination, digital strategies, information security, and statistics and data governance. Work has continued in 2021 to help reinforce the requirement that data protection issues are systematically addressed as part of the procurement and contracting processes. In particular, the Directorate for Legal Affairs has undertaken a review of the model data protection clauses, in light of recent developments in this area outside the OECD.

External Engagement and Visibility

External engagement in 2021 continued to be limited due to the COVID-19 restrictions. On 18-21 October, I participated in the 43rd meeting of the Global Privacy Assembly (GPA), a virtual meeting hosted by INAI Mexico. I continue to participate in the GPA as an accredited member in my capacity as OECD DPC, while the OECD itself has observer status.

One item of particular interest from the 2021 GPA was the adoption of a resolution on "Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes".[1] This resolution draws considerably on ongoing work by the OECD on this topic. It highlights what I continue to see as the mutually beneficial relationship between OECD and GPA.

Along with colleagues in the Directorate for Legal Affairs, the DPO participates in occasional meetings of data protection experts in international organisations to discuss topics of mutual interest. These include obstacles to the transfer of data from EEA Member States arising from the EU's General Data Protection Regulation.

Provision of Advice/Prior Consultation

The first task identified under the DPC responsibilities section of the Data Protection Rules is the provision of advice on assessing and mitigating data protection risks [Article 8.2(a)]. To that end, I have regular exchanges with the DPO on various issue that arise during his consultations with staff. In 2021, the DPO was consulted more regularly and widely by OECD staff than in 2020, most often in the context of planning or implementing new personal data processing activities.

My report last year included some indications of the types of topics on which the DPO had been consulted. In 2021 the range of topics was quite similar to that of 2020 and I have not reproduced it here. One change that could be noted from 2022, however, was a growing number of consultations regarding interviews and surveys at a national level. While the OECD has long conducted several large cross-national surveys (e.g. PISA and TALIS) the smaller scale national surveys or interviews have become much more common. These projects have diverse objectives and methodologies but might generally be seen to signify a growing appetite to have policies informed by data collected from individuals directly by the OECD or its contractors. This trend highlights the need for continued work to further strengthen a culture of data protection compliance and best practice across the policy-making sides of the Organisation.

Data Breaches

During 2021, I was notified of two minor data breaches. One breach involved the inadvertent exposure by an OECD contractor of an internal document on a developmental website during a two-hour period. The internal document included the names and functions of three OECD staff members and their association with the development of a wellness programme for the Organisation. The risks to the individuals were appropriately assessed as remote, but they were nevertheless notified about the incident.

The second breach involved the accidental inclusion of the wrong person on copy of an email to a pensioner. Affected individuals were notified and the mistakenly copied recipient confirmed deletion of the email.

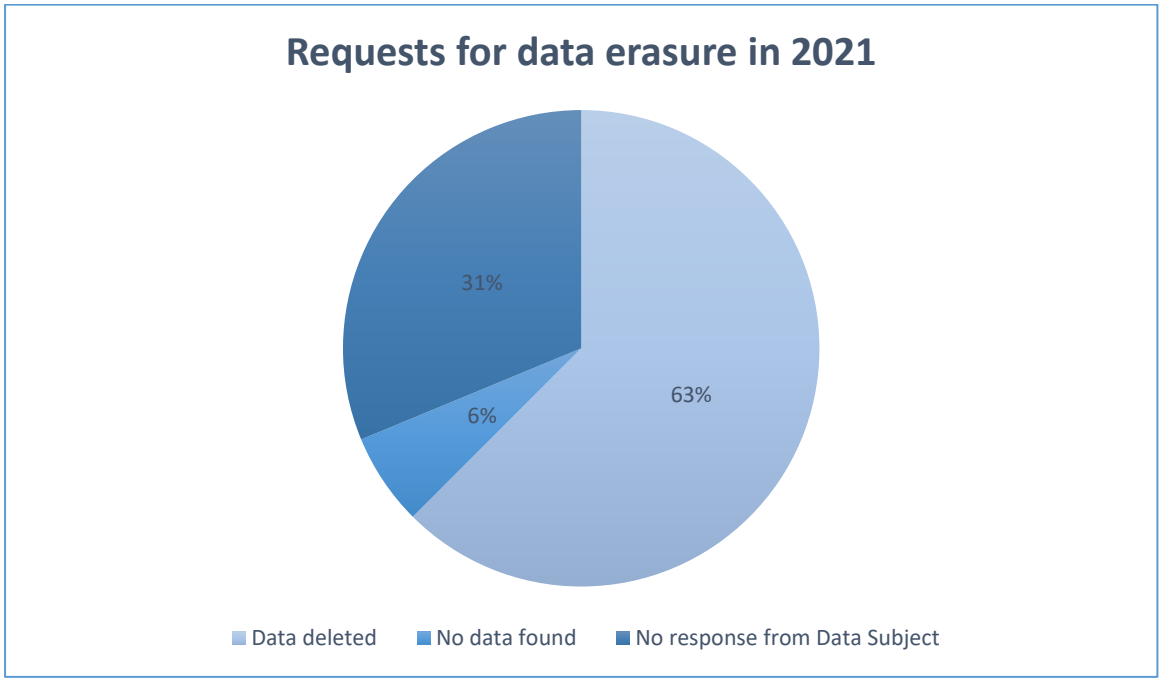
On both occasions, the incidents were handled correctly, including appropriate measures taken to reduce the risk of similar incidents in the future. I have not seen any further intervention on my part as necessary.

[1] See, https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf

Individual Rights Requests

A total of seventeen individuals submitted requests asserting individual rights under Article 5 of the Data Protection Rules in 2021. Although a few requests were sent directly to the relevant Co-ordinator, the majority were sent directly to the DPO. All but one of the requests sought erasure of personal data. For the majority of requests (10 out of 16), the personal data was deleted as requested and typically consisted of "My OECD" accounts or similar data regarding individuals who had at one time expressed interest in participating or following OECD work. In each of these cases sufficient data was provided in the request in order to enable the data to be identified and erased.

In the case of five other erasure requests, further information was sought from the requesting individual in order to determine whether relevant data was held. None of the requesters responded to the follow-up messages. It may be noted that in each of these cases the initial request was made through a third party service purporting to assist individuals to obtain data erasure. Indeed, the vast majority (12 out of 16) of erasure requests involved this third party. The recent emergence of such third-party services may explain the increase in requests during 2021 as compared with 2020 (9 received) and 2019 (3 received). While individuals are free to use such third-party services to assist them in exercising their rights, the Organisation may need to devote additional resources to address these requests if the rate of increase in requests continues.



Claims and Use of Formal Powers

In the course of the year I did not receive any claim under Article 9.1 that an individual's rights under the Rules had been infringed. No other situation arose in 2021 that required the use of my formal investigative or corrective powers under the Data Protection Rules.

The DPO received one complaint in the context of the collection of data to register for a virtual event: namely that the data sought was excessive in relation to the purpose. The DPO was able to resolve this matter satisfactorily with the event organiser and the complainant did not pursue the issue further.

International Transfers under GDPR

As I have previously noted, under the Data Protection Rules, my mandate as Commissioner is intended not only to protect the rights and freedoms of individuals in relation to the processing of their personal data by the OECD, but also to facilitate the free flow of personal data [Article 8.1(a)]. This later aspect continues to be a challenge, as the Organisation faces questions from EEA members (and contractors) about transfers of personal data 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 such as the Programme for International Student Assessment (PISA) and the Programme for the International Assessment of Adult Competencies (PIAAC), among others.

The GDPR favours a solution involving a (unilateral) decision by the European Commission that an international organisation such as the OECD ensures an adequate level of protection. I continue to believe that the OECD system demonstrably meets this requirement. Although the OECD is not subject to GDPR our EEA-based members and contractors do have to comply. An adequacy finding would be the most efficient and comprehensive solution to facilitate their continued participation in OECD work.

COVID-19 response

COVID-19 continued to impact significantly the operational side of OECD during 2021. Full-time teleworking for almost all staff and virtual engagement with delegates and participants continued for the first half of the year. As staff and limited visitors began to return to the office in in the 2nd half of the year, new arrangements were put in place to protect the health and safety of everyone on site and to ensure consistency with public health requirements in France by requiring evidence that staff/visitors have a reduced risk of transmitting the Covid-19 virus to others. More particularly all visitors were required to show the "Pass Sanitaire" to be scanned on entry. The OECD retains no records of this scan, which does not in any case indicate the precise basis on which the validity of the pass was determined. The DPO was regularly consulted prior to these measures being taken place and my advice has been sought on a number of occasions as well. As I considered the measures taken to be reasonable and proportionate, I agreed with the DPO that no objection needed to be raised to them. No complaints were received about the measures taken.

Conclusion

I am pleased to have been able to report that I was not called upon to resolve any claims of infringement of the Rules during 2021, and that the handling of individual rights requests and two data breaches was efficient. More generally, I believe that the Organisation has continued to make significant progress in enhancing the processes and controls needed to make good on the promise of the Secretary-General's 2019 Decision. Particularly notable was the launch of the eLearning course which has helped ensure that staff are fully aware of their obligations in relation to personal data. Likewise I believe the launch of Data Protection and Digital Security Focal Points will help to build and spread in house expertise in these interrelated areas across the Organisation.

As noted in my first Annual Activity Report, as we gain experience in implementing the Rules we can also reflect on how well the Rules are functioning and whether the resources and governance structures are appropriate to the task. With May 2022 set to bring the third anniversary of the new regime, I have been working with the DPO to evaluate where refinements might be appropriate. During the coming year, I expect this evaluation to conclude with recommendations as to any updates that may be needed to ensure that the overall functioning of the regime continues to merit the high

level of trust placed in the Organisation by staff and other individuals whose data is processed in furtherance of the OECD mission and programme of work.

In addition to possible updates to the data protection regime, focus in 2022 is needed on two issues that continue to be high priority:

- *Data mapping*: In co-ordination with the Digital Security Office, efforts should continue to further develop the granularity of the inventory of personal data used across the Organisation – ideally through an IT tool with greater functionality – in order to more efficiently prioritise and manage risks, respond to individual rights requests and to facilitate transparency.

- *International transfers*: Continued efforts will be needed to help EEA members address the GDPR challenges related to transfers of personal data to OECD. Convinced that an EU adequacy finding would serve as the most effective solution for EEA members, I am ready to continue raising awareness to key stakeholders on the importance of having this outcome realised. It is essential that the data flows necessary for the important public interest work of the Organisation are not unnecessarily interrupted.

These priorities are additional to the day-to-day business of providing advice to staff on compliance and good practice and responding to any individual rights requests or complaints.