OECD

ANNUAL ACTIVITY REPORT OF THE DATA PROTECTION COMMISSIONER

2020

Billy Hawkes

January 2021

Table of Contents

Introduction

This is my second report as Data Protection Commissioner (DPC), following my appointment by the Secretary-General in May 2019. My appointment served as one element of the entry into force of the *Decision of the Secretary-General on the Protection of Individuals with regard to the Processing of their Personal Data* ("Data Protection Rules") which apply 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.

The report that follows summarises the main areas where I have intervened over the past year, my actions in terms of awareness raising, and the claims I addressed and their overall results. It also provides information on the initiatives by the Data Protection Officer ("DPO") and the OECD more generally to implement the Data Protection Rules during 2020. My conclusion looks forward to plans for continuing to strengthen the regime over the course of 2021.

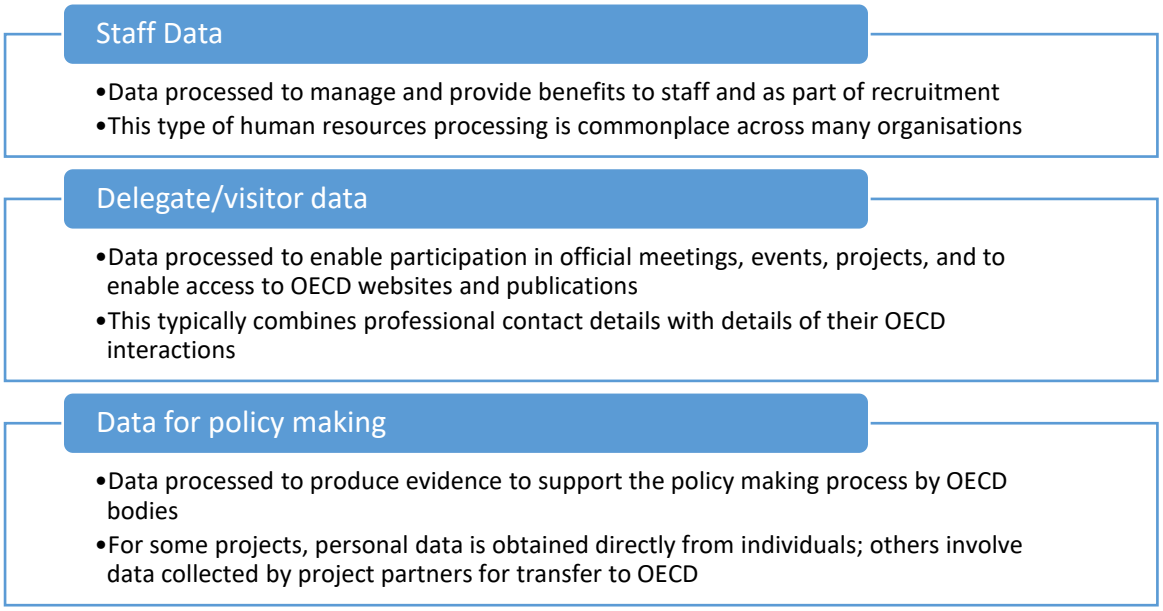
As provided by the Data Protection Rules, this report will be made available to the public on the main data protection page of the OECD website. This practice is also consistent with the longstanding focus on organisational accountability reflected in the OECD Privacy Guidelines.

Activities in 2020

Data Mapping

Efforts to comprehensively map personal data across the Organisation accelerated in 2020. Overall, the main categories of personal data are those of OECD staff, of delegates and visitors to the Organisation, and of individuals surveyed or otherwise involved in policy work.

Figure 1. Categories of Personal Data



Important initiatives in 2020 included a sensitive data discovery initiative and a statistics and governance survey which have provided useful insights. Further work is required, particularly in light of the evolving range of OECD programmes. Efforts to expand the coverage of responses to these surveys will continue in 2021. These efforts can provide a big picture view to complement the regular accumulation of insight into the Organisation's activities obtained through regular consultations by staff with the DPO and Information Technology Co-ordination Group (ITCG) for new or updated processing activities.

Information/Awareness

The Data Protection Rules includes a number of requirements related to transparency and this area has been the subject of considerable work in 2020.

Intranet/Internet

A data protection overview page on the OECD public website was created in 2019 to provide general information to the public and data subjects about the OECD's internal approach to data protection in the context of its activities. The Data Protection Rules are posted, along with my annual activity reports, my contact information and that of the DPO. Other updates to the overview page reflect additional efforts to provide transparency about the Organisation's data processing activities and associated protections.

Following a "layered" approach to the provision of information to individuals, specific notices have been posted for different activities, with the overview page serving as a hub. The separate notices address data processing in the context of visitors, recruitment, and procurement (forthcoming). These complement the OECD privacy policy which is focused on data collection in the context of visitors to the OECD website. The OECD privacy policy has been substantially overhauled and simplified in 2020 and a similar approach has been adopted for the websites across the entities within the OECD framework (such as IEA, NEA, ITF, and MOPAN) each of which has updated privacy policies. These efforts have been facilitated by the preparation of a template privacy policy to bring consistency 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 (virtual or in-person) 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.

"How to" Guides for Staff

The catalogue of "How to" guides has continued to grow, providing staff advice on compliance with the Data Protection Rules in the context of 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".

Box 1. Data Protection "How To" Guides

- Preparing a data protection notice
- Handling an individual rights request
- Handling participant lists
- Transparency and video conferencing
- Identifying personal data
- Conducting a staff survey

New guides cover, for example, transparency in the context of organising video conferences – a much more regular activity given the COVID-19 restrictions on in-person meetings. The frequency of staff surveys has also increased during COVID-19 restrictions, in order to understand the challenges posed by remote working. A new "How To" guide helps ensure that they are designed to protect the anonymity of staff who respond. Another new guide explains how to identify personal data and was prepared to address a recurring challenge for staff in understanding when their projects will use personal data and thereby bring the work within the ambit of the Data Protection Rules.

Internal Processes

New processes have been established to help ensure that data protection issues are systematically addressed as part of the procurement and contracting processes. Model provisions have been developed that can be used for both market consultations and calls for tender.

The model contract for intellectual services was updated to include a default data protection clause as well as instructions to check with the DPO where personal data is to be processed as part of the contract. For other contracts, model data protection clauses have been developed and are maintained by the Directorate for Legal Affairs. In the context of their reviews of draft contracts, staff in both the procurement and legal departments have been trained regarding the Data Protection Rules with a view to helping them identify issues and use appropriate legal provisions. Project staff are directed to consult with the DPO where this has not taken place prior to the procurement/contracting stage.

In 2020 the DPO was added as a member of the Organisation's community of Risk Focal Points, which includes representatives across the directorates in addition to the Chief Information Security Officer and Head of Ethics. Through this interaction, data protection issues can be reflected in the biannual process to update the risk register in light of evolving risks.

Internal Engagement and Visibility

A joint awareness-raising activity with the Digital Security Office was held on 28 January 2020, the first occasion on which the OECD has observed International Data Protection Day. It also provided my only opportunity during 2020 to visit the Organisation in-person due to the travel restrictions imposed shortly thereafter. The occasion included an "all-staff" message from the Secretary-General, a "Tip of the Week" communication, and the launch of several "How To" guides. The main event was the organisation of two panel discussions, focused on how strong data governance can facilitate access to the data sources needed for policymaking. I participated in the events, joining the Head of the Digital Security Office and the Acting Chief Statistician. Our discussions focused on the need for strong data governance to enable the OECD to access the data necessary for policy making. Moderated by the Head of the Digital, Knowledge and Information Service (DKI) and the Director of Science, Technology

and Innovation (STI), we highlighted to participants 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.

Follow-up communications from International Data Protection Day included a message in a February "EXD Essentials" newsletter about the need to follow the Data Protection Rules when processing personal data. It was followed in a March newsletter with a note on transparency in video conferencing, considered to be particularly timely given the surge in video conferencing associated with the onset of COVID-19.

In September, the Staff Association included a "Did you know" blurb on our data protection regime in its monthly newsletter and continues to maintain this information on its Intranet site. On 15 October, the Digital Security Office organised OECD Digital Security Day, oriented around the theme "Digital Me & We - together we are the front line for the OECD's digital security defence". Videos and a new digital security intranet page were launched to accompany a virtual panel discussion for staff. The DPO and Ethics Officer joined the Chief Information Security Officer in a session moderated by the Head of DKI that explored current security issues as well as the mutually reinforcing character of data protection, ethics and digital security to the Organisation. On 17 November, the IEA organised one of its occasional all-staff "IEAcademy" meetings around data protection. The session included a joint presentation by IEA legal staff and the DPO focused on IEA-specific data protection issues. It included as well an online quiz for participants before concluding with a question-and-answer period.

More generally, the DPO has continued his engagement with relevant co-ordination groups across the Organisation. The most active groups include the Information Technology Coordination Group (ITCG), the Statistics and Data Board at Manager's level (SDB-M), and the Statistics and Data Community of Practice on Microdata. He also stays in contact with the network of Resource Management Advisors (RMAs), Counsellors network, and Senior Communications Board with the aim of keeping a regular dialogue with colleagues particularly well positioned to identify data protection issues as they arise.

External Engagement and Visibility

External engagement in 2020 was somewhat more limited than in 2019 due to the COVID-19 restrictions. I did participate virtually in the annual workshop on Data Protection in International Organisations on 8-9 October. A key concern of participants in the workshop was the issue of new and unnecessary obstacles to the transfer of data from EU Member States arising from the General Data Protection Regulation and the restrictive interpretation of its terms promulgated by the European Data Protection Board. I comment further below on how this issue impacts on OECD programmes.

The following week, on 13-15 October, I participated in the 42nd meeting of the Global Privacy Assembly, also held virtually. A key take-away from the Assembly was the successful efforts of data protection authorities to come up with approaches to COVID-19 challenges that reconciled the public health and data protection issues. On both occasions, I was joined by the DPO and other OECD colleagues working on data protection issues.

Provision of Advice/Prior Consultation

Under the Data Protection Rules, it is the primary role of the DPO to assist Coordinators[1] with compliance responsibilities, and I provide advice to the DPO through regular exchanges on particular issues. During 2020, the DPO was consulted on a large number of projects from across the

[1] Under the Data Protection Rules, Coordinators – typically Directors or Heads of Service – are held accountable for the processing of personal data

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.

Box 2. Selected Topics of DPO Consultations (2020)

meeting webcasts · events app · staff mobile phone charges · candidate screening tools · public consultations · survey on gender · CRM tool · staff training · service desk contract · access to staff accounts · student surveys · teacher surveys · events app · use of expert's data · survey of farmers · health microdata survey · survey of consumers · 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 · survey on AI · social listening tools · learning assessment platform · survey of firms · interviews for education review · internet user survey · survey of trust · recruitment tools · financial literacy survey ·interviews for migration survey

Data Breaches

During 2020, I was notified of two data breaches, both of which I consider to be relatively minor. Both involve entities/bodies within the OECD framework, who are subject to the OECD Data Protection Rules and therefore my oversight.

One breach involved the International Energy Agency and resulted from the inadvertent inclusion of a list of email addresses sent as part of a group email. The addresses in the document were identical to those of the email recipients, all of whom were notified and requested to delete the attachment.

The second breach involved the International Service for Remunerations and Pensions, which inadvertently sent a small number of payslips, which included financial details, to the wrong pensioners. Affected individuals were notified.

On both occasions, appropriate measures were taken by the responsible bodies on their own account to reduce the risk of similar incidents in the future, and I have not seen any intervention on my part as necessary.

Individual Rights Requests

Ten requests asserting individual rights under the Data Protection Rules were received by the DPO in 2020. Nine of the requests sought deletion of personal data, each of which was complied with by the Coordinator. One request sought confirmation as to whether an individual's data had been transmitted between tax authorities through the Common Transmission System (CTS). The security architecture of the CTS is designed to ensure that only the sending tax authority can encrypt, and only the intended receiving tax authority decrypt the tax information transmitted. As a result of this design, the DPO was unable to confirm to the requesting individual whether or not personal data had been processed. I reviewed the handling of this request and found it appropriate under the Data Protection Rules. Summary details of a related complaint about the CTS from the same individual are given below.

Claims and Use of Formal Powers

Two claims were submitted to me in 2020, one from a staff member in relation to an internal process involving disclosure of personal data, the other from an outside lawyer challenging the OECD's role in the area of international activity to combat tax evasion.

Personnel Issue

A staff member submitted a claim that sensitive data – notification of future absence due to maternity – was automatically conveyed via an internal electronic resource management system to other members of staff in her Unit. She did not consider such notification to be necessary for the purposes of the Organisation.

I raised this issue with the relevant Coordinator – in this case, the Executive Director – indicating that I was investigating the complaint under the Organisation's Data Protection Rules. The Coordinator's response included a change to the text of the notification so that the reason for absence in such cases would no longer be explicit. In parallel, the DPO wrote to all Coordinators requesting that they review the list of staff with access to such notifications with a view to reducing the list to the minimum required.

I conveyed this outcome to the staff member who indicated that I could consider her complaint satisfactorily resolved by the actions taken.

I consider the outcome in this case to be a positive indication of the willingness of Coordinators to adjust standard procedures where this is desirable to ensure better alignment with the Data Protection Rules.

OECD Role in International Activity to Combat Tax Evasion

A lawyer acting on behalf of clients submitted a claim that the activities of the OECD Centre for Tax Policy in facilitating exchange of tax information on individuals with a view to combating tax evasion – and specifically, the Common Transmission System (CTS) provided by OECD as a service to participating jurisdictions – were in breach of the Data Protection Rules.

I raised this issue with the relevant Coordinator – the Director of the Centre for Tax Policy and Administration – and invited his comments. I also independently analysed the complaint by reference to the Rules and invited both the Complainant and the Coordinator to comment on this analysis and my preliminary conclusions of a factual nature. Having taken account of these comments, I reached the following Conclusions:

- The Coordinator is accountable for compliance with the requirements of Article 4.1 of the Rules for the personal data of individuals in participating jurisdictions held by OECD/CTPA in relation to the operation of the CTS and has discharged this responsibility in accordance with the Rules
- The Coordinator is accountable for compliance with the requirements of Article 4.1 c) of the Rules in relation to the operational security of the CTS and has taken sufficient measures to discharge this responsibility in accordance with the Rules
- The Coordinator is not accountable for the personal data of individual taxpayers transmitted through the CTS and thus not obliged to comply with the Rules in relation to such data.

I also offered the following general advice:

- Before involving itself in programmes involving significant processing of personal data, a Coordinator should ensure that a thorough Data Protection Risk Assessment is carried out, in consultation with the Data Protection Officer, in accordance with Article 6.2 of the Rules
- Subject to relevant security considerations, the maximum transparency vis-à-vis the public should be ensured through extensive publication of the details of such processing, and any underlying agreements, on the OECD website.

International Transfers under GDPR

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. This later aspect has become a growing challenge, as the Organisation faces questions from EEA members 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 like the Programme for International Student Assessment (PISA) and the Programme for the International Assessment of Adult Competencies (PIAAC), but in a number of other projects as well.

As I noted in my report last year, 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 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-based members and contractors do have to comply.

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 believe that the OECD system demonstrably meets this requirement. In the absence of such a decision, OECD has been exploring other options contained in the GDPR to assist its EEA Members who are reluctant to use the "public interest" derogation contained in the GDPR in view of the restrictive interpretation placed on this derogation by the European Data Protection Board. I will continue to support the DPO and the Directorate for Legal Affairs in their efforts to find appropriate solutions to ensure that the data flows necessary for the important public interest work of the Organisation are not unnecessarily interrupted.

COVID-19 response

No reporting on 2020 could avoid mention of COVID-19, which has impacted significantly the operational side of OECD. Since early March, nearly all staff have been teleworking full-time and all engagement with delegates and participants has become virtual. Early in the crisis, OECD management took steps to enable the organisation to adapt its functioning as the pandemic unfolded and has evolved its strategy and measures as the situation evolved.

In some cases these measures involved processing personal data, for example to address health and safety risks when a staff member or visitor reported having medical confirmation of a positive COVID-19 test. Likewise, even after the Organisation was closed to all but essential workers, protocols were put in place to screen any staff or visitor to the Organisation. As almost all interactions moved virtual, data protection notices and other transparency tools have been updated to ensure that staff and outside participants were aware of how their data was captured and used. These have been

complemented by enhanced digital security measures to address an elevated risk environment during the crisis. The DPO has been regularly consulted prior to these measures being taken place and my advice has been sought on a number of occasions as well.

Conclusion

Looking back, I believe we have made substantial progress over the past year to enhance the processes, tools and controls needed to make good on the promise of the Secretary-General's 2019 Decision. In particular, advances can be reported in two of the areas highlighted as priorities for 2020 in my annual report last year.

One priority focused on updating data protection notices as part of our layered notice approach to transparency. Considerable work was done in this area and there is now a broad and consistent approach across the OECD and affiliated bodies.

A second priority area was data breach incident response. The Digital Security Office released and publicised a "How To" guide, in co-ordination with the DPO. Where the incident concerns personal data, the Guide closely tracks the requirements of the Data Protection Rules and this issue continues to benefit from regular review and assessment as part of OECD's processes to manage risk.

Although progress was made across the three other priority areas identified for 2020, a continued focus is needed in 2021, and likely beyond. These include:

- *Data mapping*: In co-ordination with the Digital Security Office, continued efforts are needed to further develop the inventory of the personal data uses across the Organisation and make the outcomes transparent.
- *Awareness-raising and training*: Early in 2021, International Data Protection Day activities will again serve as a further opportunity to raise awareness about the Rules. Plans for introducing further training activities should also be operationalised, ideally integrating data protection with digital security and co-ordinated with other OECD training programmes.
- *International transfers*: Continued efforts will be needed to help EEA members address the GDPR challenges related to transfers of personal data to OECD. I intend to continue drawing attention to the importance of addressing this issue to key stakeholders inside and outside the 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.