OECD

ANNUAL ACTIVITY REPORT OF THE DATA PROTECTION COMMISSIONER

2023

Billy Hawkes

January 2024

Table of Contents

Introduction

This is my fifth 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.

There were no changes to the legal framework in 2023, nor complaints or other incidents requiring the use of my formal powers for me to report on this year. One notable development, however, has been the first instance in which the organisation has been called upon to implement new transparency requirements related to the use of artificial intelligence. The requirements were introduced through changes in the Rules introduced in 2022. Also noteworthy, was the conclusion of a sensitive data inventory, which has brought greater insights into the Organisation's data processing practices.

These developments are described below, along with a summary of other activities including the initiatives taken by the Data Protection Officer (DPO) and the OECD more generally. My conclusion includes some reflections on progress made as we approach the five-year anniversary of the Data Protection Rules under which I was appointed Commissioner.

As required 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 2023

Internal Engagement and Processes

This section describes Organisation-wide initiatives to implement the Data Protection Rules. It does not cover the regular work to ensure that data protection rules are fully reflected in specific projects involving the processing of personal data. In that respect, I have regular consultations with the DPO, who in turn provides the advice to staff members that is crucial to maintaining a high standard of data protection.

Data Mapping

My annual reports have regularly noted the importance of having a broad view of the processing of personal data across the organisation, a topic specifically addressed in the Privacy Management Programme adopted by the Secretary-General in 2022. Working closely with the Digital Security office, in 2023 the DPO conducted an inventory exercise covering personal and other sensitive data processed by the Organisation. There remains work to be done to analyse the results, re-assess risks, and keep the records updated. However, this effort reflected considerable work by directorates and represents a substantial advance on the record keeping required under the Rules and the Privacy Management Programme. Credit should also be extended to the Data Protection and Digital Security Focal points, who co-ordinated responses on behalf of directorates.

Artificial Intelligence

On the policy side, the OECD has been at the forefront of Artificial Intelligence (AI) governance, with its 2019 Council Recommendation, the first intergovernmental standard on this topic. That

Recommendation recognised the positive transformational implications of AI but also the importance of respecting privacy and data protection, with specific provisions on transparency and explainability. The AI Recommendation inspired modifications to the OECD Data Protection Rules proposed by myself and the DPO and adopted by the Secretary-General in 2022. In particular, the modifications impose new transparency requirements and provide individuals a new right to challenge certain AI outcomes.

Nearly immediately, the new AI provisions were implicated by the use of an AI system in the context of recruitment of young professionals (the Young Associates Programme) at the OECD. As a result, the Organisation updated its Data Protection Notice for Recruitment to reflect the use of a service provider using AI to help screen applicants. More generally, the Organisation has been actively adapting working practices to take advantage of the potential of generative AI tools. The use of these tools raises a number of risks, including in relation to data protection and digital security, as a result of which the Organisation has established new internal guidelines to help staff identify and mitigate these risks. This is a challenging and fast-moving area that I am monitoring closely with the assistance of the DPO.

Data Protection and Digital Security Focal Points

The network of Data Protection and Digital Security Focal Points met quarterly in 2023, with participation from every OECD Directorate as well as the IEA, NEA, and ITF. Focal points serve as privacy/security 'champions' across key business functions, working with the DPO and the Digital Security Office to improve communication channels, identify privacy and security issues raised by day-to-day work, and embed good practices as part of the Organisation's workplace culture. As anticipated, the network has built the Organisation's expertise and capacity, and was helpful in co-ordinating responses to the Sensitive and Personal Data inventory exercise as noted above.

Information/Awareness

Data Protection Day in January 2023 was marked by an "All Staff" message from the OECD Secretary-General. His message both recalled the recent achievements and announced upcoming initiatives. On the policy side, he noted a new intergovernmental agreement on common approaches to safeguarding privacy when accessing personal data for national security and law enforcement purposes, in the form of the OECD *Declaration on Government Access to Personal Data Held by Private Sector Entities*.

In terms of OECD internal practices, he announced the release of new guidance on data protection in the context of procurement and contracting, as well as an updated set of model data protection clauses for inclusion in contracts that involve the processing of personal data. The Data Protection Day message also directed staff to the newly-released Data Protection Notice for Staff Data, which describes the various types of staff data processed and purposes for which it is used. It further includes a list of service providers relied on by the Organisation in processing staff data as well as the tools and mechanisms that exist for staff to access and correct their information or otherwise assert data protection rights. Finally, the Secretary-General encouraged staff co-operation in completing the Sensitive Data Inventory.

Other awareness initiatives during 2023 included a message in the "EXD Essentials" newsletter promoting the guidance on procurement and contracting. Additionally, a "Tip of the Week" message highlighted the work of the Data Protection and Digital Security Focal Points to all staff.

External Engagement and Visibility

I represented the OECD at two data protection events during 2023. In early October, I was joined by a colleague from the policy-side of OECD in the 45th meeting of the Global Privacy Assembly (GPA) in Bermuda. I continue to participate in the GPA as an accredited member in my capacity as OECD Data Protection Commissioner, while the OECD itself has observer status.

Later in October, I joined the DPO and colleagues from the OECD Legal Affairs Directorate in Lyon, France at the annual Workshop on Data Protection within International Organisations. Hosted by Interpol, with the support of the European Data Protection Supervisor, this meeting proved an excellent opportunity to exchange on topics of common interest with our colleagues in other international organisations. I was pleased to moderate a session on biometrics. The DPO spoke during a panel on risk management, highlighting OECD experiences in implementing its new AI provisions.

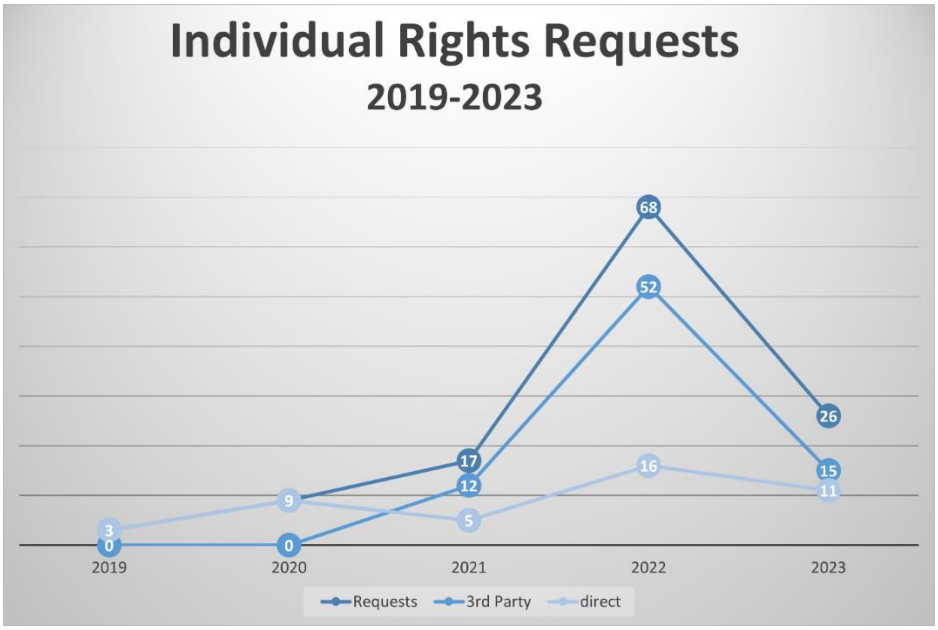
Data Breaches

No data breaches were notified to me or the DPO in 2023.

Individual Rights Requests

During 2023 a total of 26 individuals submitted requests regarding their personal data, which were treated as requests asserting individual rights under Article 5 of the Data Protection Rules. Although a few requests were sent directly to the relevant directorate, the majority were sent to the DPO. Twenty-two of the requestors sought erasure of personal data, and 4 sought access to their data.

As compared with 2022 – which saw a dramatic increase in rights requests – 2023 reflected a return to a more typical level of rights requests. This dynamic is attributable to a significant reduction in the third-party requests that caused the spike in 2022. Of the requests for erasure, nearly one-half could be resolved (with data deleted) on the basis of the request alone. For the others, further information about the request was sought from the requester. As in 2022, none of the requesters responded to the follow-up messages. On the whole, it remains the case that third party services are the primary driver of individual rights requests to the OECD.



Claims and Use of Formal Powers

In 2023, I did not receive any claim under Article 9.1 of the Data Protection Rules that an individual's rights had been infringed or other failure to comply with the Rules. Nor did any other situation arise in 2023 that required the use of my formal investigative or corrective powers under the Rules.

International Transfers under GDPR

Each of my previous annual activity reports has discussed the challenges facing the Organisation that result from questions raised by 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). In that sense, the issues are not unique to the OECD and there has been interest among a number of international organisations in working with EU stakeholders to address the issue, with several approaches under consideration that attempt to take into account the status of international organisations.

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 and that an adequacy finding would be the most efficient and comprehensive solution to facilitate the continued participation of our EEA-based members and contractors in OECD work.

Conclusion

Once again, I am pleased to have been able to report that the past year brought neither claims of infringement nor data breach notifications. Likewise, the data mapping progress reflected by the completion of the work on the Sensitive Data Inventory is an important milestone for the organisation in its implementation journey and responds to the priorities I have identified in past reports.

We are approaching five years since the adoption of the Data Protection Rules under which I was appointed Commissioner. Each of my prior reports has included a list of priorities for the organisation. With the completion of the first sensitive data inventory, the only remaining topic from my list from past years remains the issues around international transfers. In 2024, I will continue to raise awareness to key stakeholders on the importance of having an appropriate solution to the transfer issue – which I believe to be an adequacy finding – to ensure that the personal data flows necessary for the important public interest work of the Organisation are not unnecessarily interrupted.

Rather than identifying new priorities for the organisation, I will conclude my report this year with a point regarding the overall approach of the Data Protection Commissioner to ensuring oversight for a regime like that of the OECD. Led by the DPO, the Organisation has worked successfully since 2019 to put in place the essential elements of an implementation framework (as specified in the Privacy Management Programme). I have been pleased to provide advice and help shape that work. With that framework now in place, I intend to take a more pro-active role in the coming year to ensure that it is working effectively in practice in selected data processing activities across the organisation.

I conclude by observing that data protection policy and practice continue to evolve at a rapid pace, and the OECD will need to continue to review and adapt the regime as needed to ensure that it meets the expectations of its members and the individuals whose data is entrusted to the Organisation in furtherance of its work.