OECD

ANNUAL ACTIVITY REPORT OF THE DATA PROTECTION COMMISSIONER

2022

Billy Hawkes

January 2023

Table of Contents

Introduction

This is my fourth 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.

In October of 2022, the OECD Secretary-General adopted revisions to the Data Protection Rules, on my recommendation, put forward jointly with the Data Protection Officer (DPO). At the same time, he adopted a Privacy Management Programme, framed as implementation Guidelines. These developments are described below along with a summary of other activities including the initiatives taken by the DPO and the OECD more generally. As in my 2021 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.

Revisions to the Data Protection Regime

Going back as far as 1992, the OECD has had binding rules governing the processing by staff of personal data. Following consultation with the Staff Association, the Rules were strengthened considerably in 2019, with stronger rights for individuals and the creation of a new governance structure including the establishment of my role and that of the DPO.

Three years of experience in applying the 2019 OECD Data Protection Rules indicated that their basic structure and principles were sound, and considerable work has been done across multiple fronts to implement the Rules. No complaints to date have required me to use my corrective powers under the Rules. Details are documented in my Annual Activity Reports.

Revisions to the Data Protection Rules

Nevertheless, the experience to date did suggest that aspects of the Data Protection Rules would benefit from refinement and improvement. This possibility is envisaged in the Decision itself, which provides that it may be amended at any time [Art. 10(c)]. Following internal consultations as well as with the Staff Association, together with the DPO I proposed revisions to the Secretary-General intended to: (1) ensure a high level of protection to the individuals whose data we process, (2) better tailor the Decision to the data processing activities of the Organisation, and (3) help meet the evolving expectations of OECD members and other partners who entrust the Organisation with personal data that is essential to its work.

The revised text was adopted by the Secretary-General, as proposed, and went into effect on 28 October 2022. Some of the changes reflect the latest OECD policy advice. For example, there are new rules on artificial intelligence following the OECD Council Recommendation on this topic. Other changes were inspired by experience with complaints I have had to resolve. For example, the Rules now make explicit that they apply when the OECD acts as a data processor for another data controller. In still other areas, the Rules just needed some tailoring to ensure a better fit for purpose. A provision on data portability was removed because it did not apply well to the type of data OECD processes. The

breach notification timing was changed from 48 hours to 72 to be better adapted to the regular business practices of the OECD's service providers and done in a manner that does not undermine the basic protections for individuals. The provisions on sensitive data (reframed as "special category data") were expanded to include data regarding criminal convictions or allegations as well as ethnicity. Rules regarding transfers outside the Organisation were refined to ensure that transferred data benefits from the same high standards applied to data held by the Organisation. The revised Rules clarify that – although the OECD itself is considered the data controller – within the Organisation, responsibility for compliance is assigned at the level of Director.

The revised Rules retain the clause requiring a review after five years, and we will continue to monitor the ongoing effectiveness of the Rules, with an eye as well to the continuing evolution in data protection policy and best practice.

Adoption of a Privacy Management Programme

A Privacy Management Programme is the basic building block of an accountable organisation, as recommended by the OECD Council in the 2013 revisions to the OECD Privacy Guidelines (paragraph 15). The OECD Privacy Management Programme, adopted by the Secretary-General as 'Implementation Rules' under Article 10(b) of the Data Protection Rules, describes the OECD approach to implementation in a number of important areas. These include risk assessment, procurement and contracting, data subject requests, staff training, risk management and transparency. The Privacy Management Programme also highlights how the data protection function has been integrated across regular business activity, including through the establishment of data protection focal points, which is critical to maximising impact and leveraging resources.

The OECD Privacy Guidelines call for accountable organisations to be prepared to demonstrate as necessary for oversight, and in its own practice the Organisation has taken this a step further by making its Privacy Management Programme public. It is to be reviewed every two years.

Activities in 2022

Internal Engagement and Processes

A number of developments in 2022 demonstrate a continued commitment to implementation of the Data Protection Rules. This section describes these developments, which cover Organisation-wide initiatives and not data protection in specific projects. More generally, I was happy to note that the DPO – with whom I have regular consultations – was actively involved in ensuring that the Data Protection Rules were fully reflected in OECD activities, notably new projects that sometimes raised complex data protection issues. I see this as evidence that his role – new to the Organisation – is now fully embedded in the structure of the Organisation.

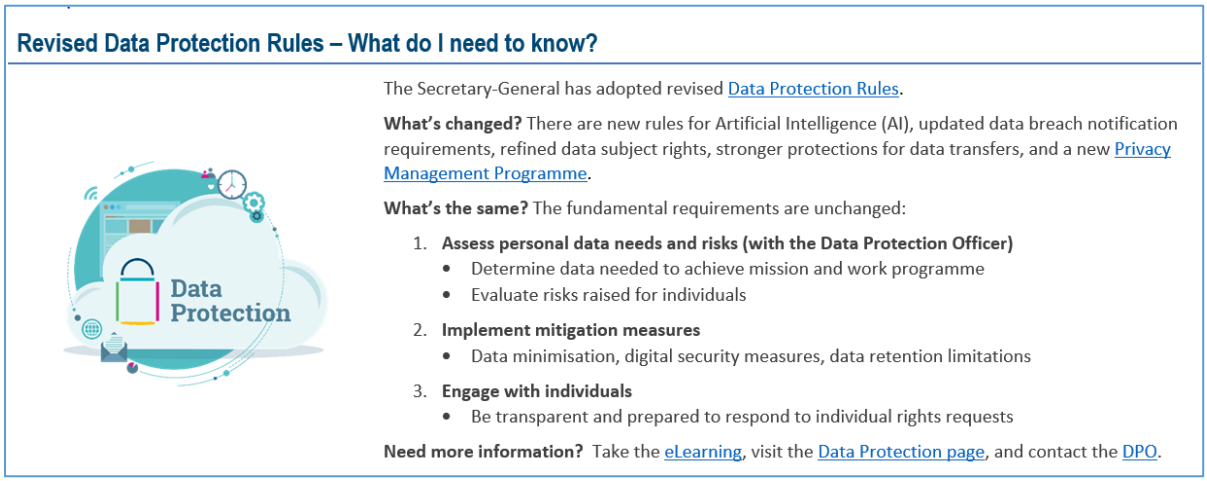
Data Protection and Digital Security Focal Points

Last year saw the formal launch of a new network of Data Protection and Digital Security Focal Points. Recognising that organisational change is difficult, this initiative embeds privacy/security 'champions' across key business functions. Designated by each directorate/service, the focal points work 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. The launch follows a successful pilot phase conducted earlier in 2022 and I expect the new network will help build the Organisation's expertise and capacity, expanding a culture of privacy and digital security across the Organisation.

Information/Awareness

An important development in the provision of information was the conclusion of work to develop a comprehensive data protection notice for staff data. Until now, information about staff data uses was distributed across multiple information sources, and this effort brings together in a single document 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.

Awareness raising in 2022 included two "All Staff" email messages and an item in "EXD Essentials" which is an occasional newsletter sent to all staff. In January, the DPO sent out an "All Staff" message, circulating my annual activity report for 2021 and encouraging staff to take the data protection eLearning. In November, following his adoption of the revised Data Protection Rules, the Secretary-General sent an "All Staff" message to announce the changes. This message was followed by a communication in the EXD Essentials newsletter (see below) focused on raising awareness about the key changes in the rules as well as recalling the fundamental requirements for data protection compliance (which remained unchanged).



Revised Data Protection Rules – What do I need to know?

The Secretary-General has adopted revised Data Protection Rules.

What's changed? There are new rules for Artificial Intelligence (AI), updated data breach notification requirements, refined data subject rights, stronger protections for data transfers, and a new Privacy Management Programme.

What's the same? The fundamental requirements are unchanged:

1. **Assess personal data needs and risks (with the Data Protection Officer)**
   - Determine data needed to achieve mission and work programme
   - Evaluate risks raised for individuals
2. **Implement mitigation measures**
   - Data minimisation, digital security measures, data retention limitations
3. **Engage with individuals**
   - Be transparent and prepared to respond to individual rights requests

Need more information? Take the eLearning, visit the Data Protection page, and contact the DPO.

Other awareness raising initiatives resulted from continued close co-operation with the Digital Security Office. The focus of Digital Security Day 2022 was data breach response, an excellent choice from a data protection perspective. Data protection elements were integrated across the various initiatives wherever relevant, including in the quiz, video, and digital security game designed for small groups to explore the impacts of a data breach and how to respond. Also welcome was the encouragement to complete the data protection eLearning, which was reflected in Digital Security Day communications.

External Engagement and Visibility

With the lifting of Covid-related travel restrictions, I was again able to represent the OECD in data protection community events during 2022. In May, I participated in a workshop on data protection within international organisations, hosted by the World Food Program in Rome. This is an annual event organised by the European Data Protection Supervisor and 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 data subject rights and found the exchange of good practice instructive.

In October, I was joined by the DPO and colleagues from the policy-side of OECD as participants in the 44th meeting of the Global Privacy Assembly (GPA) in Istanbul. 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.

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 among other issues.

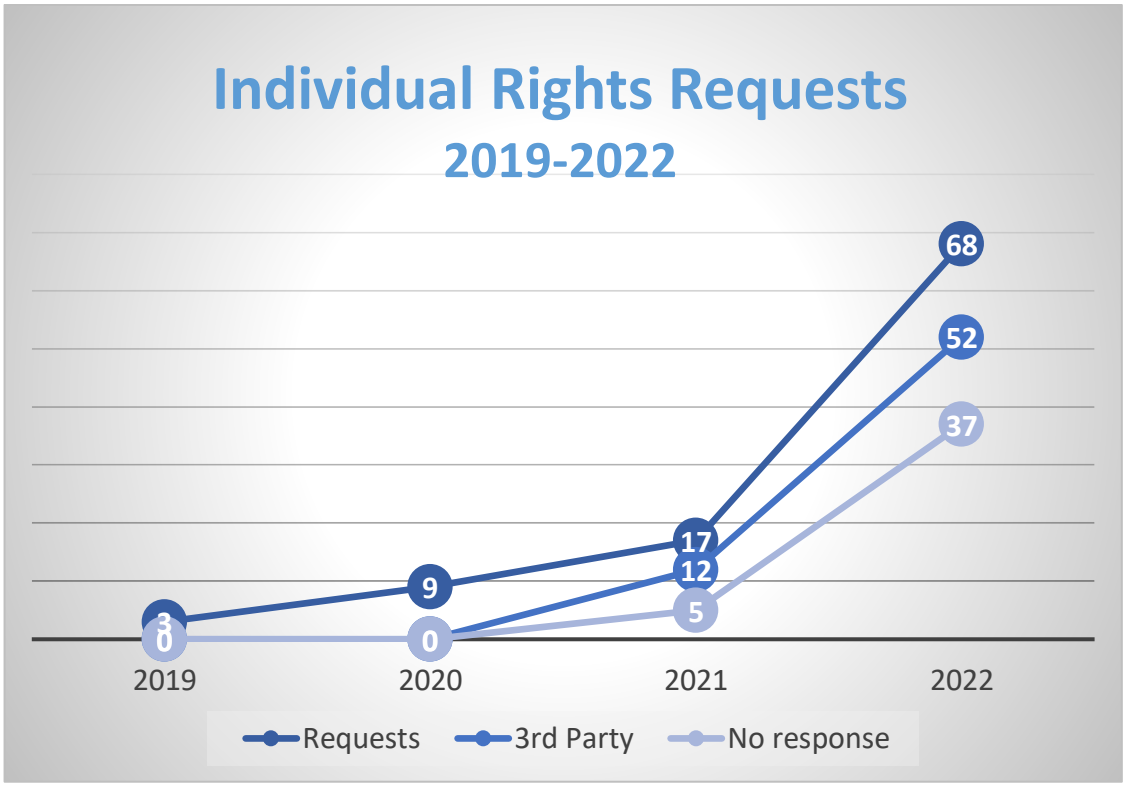
Data Breaches

No data breaches were notified to me or the DPO in 2022.

Individual Rights Requests

A total of 68 individuals submitted requests which were treated as requests asserting individual rights under Article 5 of the Data Protection Rules in 2022. Although a few requests were sent directly to the relevant directorate, the majority were sent to the DPO. Two requests were for access with the remainder seeking erasure of personal data.

As seen in the table below, a significant majority of requests (52) were made through a third-party service purporting to assist individuals to obtain data erasure. For some of these requests (15), data was identified and erased. For the majority (37), however, further information was sought from the requesting individual to determine whether relevant data was held. None of the requesters responded to the follow-up messages.



As is also reflected in the table, 2022 brought a significant growth in individual rights requests over the preceding three years, nearly all attributable to the use of third-party services. It's not entirely

clear how to interpret the fact that so many individuals did not reply to the follow-up requests, other than to suggest that those using third-party services do not demonstrate the same interest in the process as those who do not. I reiterate my comment from last year that, although 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 increase in requests continues.

Claims and Use of Formal Powers

In the course of 2022, I did not receive any claim under Article 9.1 of the Data Protection Rules that an individual's rights had been infringed. No other situation arose in 2022 that required the use of my formal investigative or corrective powers under the Rules. In one instance, an individual contacted me following a request for erasure when his request was not fully implemented (he had not been removed from a mailing list for one OECD directorate). This mistake was resolved by the Directorate in question and the individual was satisfied with the explanation.

International Transfers under GDPR

My annual activity reports have repeatedly recounted 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.

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. Revisions in 2022 that further strengthen the Data Protection Rules only reinforce this belief. 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 I was not called upon to resolve any claims of infringement of the Rules during 2022. Nor did the year bring any data breach notifications. The adoption of updated Rules and the new Privacy Management Programme equips the OECD with a legal regime that provides robust protections to individuals, as befits a body with a distinguished history of policy leadership in the area. Likewise, the regime is now better tailored to the day-to-day work of the Organisation which I expect to further facilitate effective implementation. 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.

Effective implementation is as important as the legal framework. One dimension to highlight is the close co-operation in 2022 between the data protection and digital security functions. The decision to focus Digital Security Day on data breach response was welcome as was the effort to embrace the data protection dimensions of the issue. This co-operation was fully evident as well in the work to support the Data Protection and Digital Security Focal Point network which is expanding expertise and capacity across the Organisation. The co-operation could be seen to extend more broadly between

the data protection function and all services within the Executive Directorate, as reflected in the work on the new data protection notice for staff data.

Looking ahead, further focus in 2023 is needed on two issues that continue to be high priority:

- **Data mapping**: The new Privacy Management Programme recalls that strong record keeping practices are a foundation for data protection compliance, as well as facilitating the Organisation's capacity to prioritise and manage risks. To ensure an Organisation-wide view, the DPO is given responsibility for synthesising the directorate-level record-keeping into a more comprehensive inventory. With a view to efficiency and consistency, the Privacy Management Programme further calls for co-ordination with other inventory activities within the Organisation. This vision should be fully realised in 2023, with work by the DPO, together with the Digital Security Office and other parts of the IT service to enable the directorates to integrate their record keeping efforts in a harmonised way.

- **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 will continue to raise 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 broader set of commitments reflected in the Privacy Management Programme and the day-to-day business of providing advice to staff and responding to any individual rights requests or complaints.