Europäisches Patentamt
European Patent Office
Office européen des brevets

Data Protection Report 2024

Annex to the Annual Review

epo.org

Executive summary

In 2024 the EPO pursued the consistent application of data protection standards and principles through the activities of the Data Protection Office (DPO), the Data Protection Liaison network and the delegated controllers, with the support of the Data Protection Board. This followed the adoption of a new personal data protection framework in 2022 and the implementation of numerous operational instruments in 2023.

This was achieved by engaging in the progressive operationalisation of the privacy-by-design principle, fostering and maintaining a strong culture of transparency and accountability in the processing of personal data and sustaining constructive and beneficial innovation, all while keeping people at the heart of technological developments.

With the aim of further strengthening compliance and triggering a positive cycle of improvement, the DPO conducted data protection audits and optimised existing data protection risk assessment instruments. This enabled the Office to adequately assess, manage and mitigate potential risks to the rights and freedoms of data subjects. Through the creation and continuous updating of appropriate instruments and procedures, the DPO further supported the Office's operational units in detecting and addressing personal data breaches, and analysing the root causes of detected incidents with a view to preventing recurrence.

In line with the Strategic Plan 2028 (SP2028) and the DPO Strategy and Planning 2024-2026, initiatives were introduced to support the data protection-compliant integration of emerging technologies into the Office's business operations. These included awareness-raising events organised by the DPO on data protection using artificial intelligence (AI) and specific training for Data Protection Liaisons to prepare them for future challenges.

Throughout 2024, the DPO continued to provide guidance on the interpretation of the Data Protection Rules and support to internal and external data subjects, while monitoring the implementation of the instruments created for the exercise of data protection rights. Furthermore, reflecting the cross-functional nature of data protection within the Office's structure, the DPO provided independent advice contributing to numerous projects across different areas.

The DPO also promoted numerous training initiatives, introducing new guidance documents and e-learnings to enhance the expertise of the Data Protection Liaisons, in view of their key role in ensuring the operational compliance of the Office. These enable them to effectively support delegated controllers in embedding data protection requirements into daily business operations.

Leading by example, the Office, through the DPO, further strengthened co-operation with other international organisations and European institutions in the area of personal data protection. The DPO actively participated in working groups with the European Data Protection Supervisor and other international organisations, fostering exchange and alignment on best practices for safeguarding personal data. Close collaboration with the Data Protection Board was also reinforced to advance the implementation of the EPO data protection framework across the entire Organisation.

Contents

1. Introduction

The Office fosters a culture of compliance, ensuring that personal data and privacy are safeguarded by everyone across all policies and practices. Accountability and respect for fundamental rights should guide all activities involving the processing of personal data.

The DPO serves as the focal co-ordination point for all activities related to privacy and personal data protection, in line with SP2028 and the DPO Strategy and Planning 2024-2026. The DPO has five main areas of competence:

- **Monitoring and supervision**: the DPO monitors compliance with the Data Protection Rules (DPR) in the processing of personal data, assesses technological developments impacting the protection of personal data, and performs data protection audits and investigations.
- **Risk management**: the DPO provides the appropriate instruments and supports controllers and delegated controllers in assessing and mitigating risks related to the processing of personal data.
- **Policy and advisory**: the DPO independently advises the President of the Office, the President of the Boards of Appeal and the Administrative Council on legislative proposals and initiatives involving data protection aspects and the interpretation of the DPR.
- **Training and awareness raising**: the DPO organises training and awareness-raising initiatives on data protection and ensures that data subjects are informed of their rights and how to exercise them.
- **Co-operation**: the DPO co-operates with internal and external stakeholders (international organisations, European institutions, and data protection networks) in various projects and works closely with the Data Protection Board (DPB), for which it provides a secretariat.

The DPO is supported by the network of Data Protection Liaisons (DPLs), who provide direct operational assistance to the operational units in complying with their obligations under the DPR.

Figure 1 – DPO strategy

Source: EPO

This annual report, which under Article 43 DPR is submitted annually by the DPO to the Administrative Council, the President of the Office and the President of the Boards of Appeal, highlights the DPO's activities in 2024, focusing on the results achieved in line with SP2028 and the DPO Strategy and Planning 2024-2026.

Key highlights from the Office's activities in the area of privacy and data protection in 2024 include:

- **Enhanced compliance**: the DPO conducted a higher number of data protection audits, significantly increased the number of data protection risk assessments, streamlined its risk management procedures, and maintained continuous focus on the detection, management and mitigation of personal data breaches.
- **Integration of new technologies**: in alignment with SP2028, the DPO promoted numerous initiatives supporting the integration of new technologies such as AI in the EPO's business operations and organised trainings and awareness-raising events on data protection and AI.
- **Improved services**: the DPO continued to provide independent advice to operational units and data subjects, with almost 400 consultations on a large variety of data protection related topics.
- **Enriched awareness raising**: new guidance documents were published by the DPO, and a new e-learning was launched. The DPO also delivered extensive training to the DPLs through a comprehensive support and enhancement programme designed to allow the DPLs to competently assist the delegated controllers in daily business operations across all areas of data protection. The new "DPO Highlights" were launched to raise awareness among staff about new data protection instruments and procedures in the Office, as well as important updates from the international data protection landscape.
- **Strengthened co-operation**: the DPO was involved in a growing number of joint projects with other EPO units, while co-operation with international

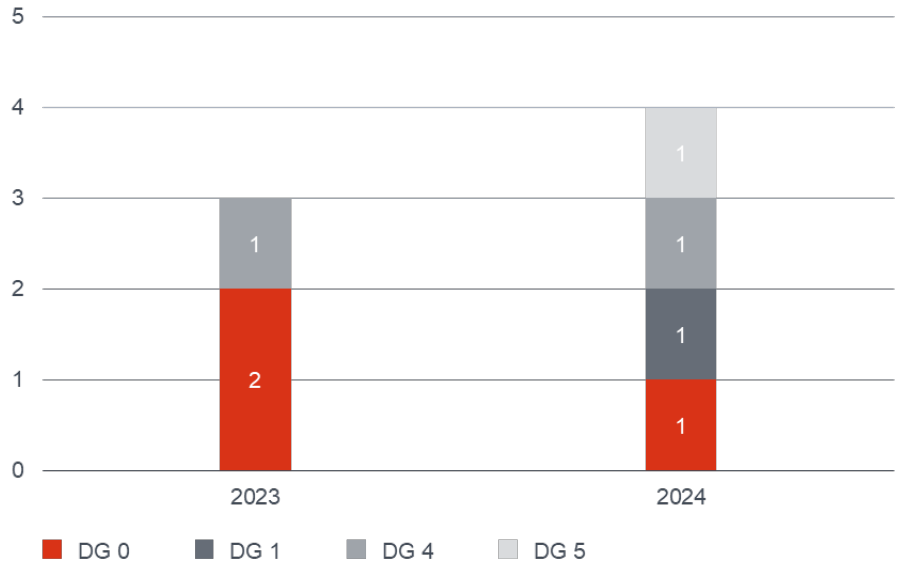
organisations and European institutions was also strengthened and enhanced. The DPO also supported co-operation with the national patent offices in the implementation of the Digital Toolkit. A network of DPOs of international organisations was launched, with the aim of knowledge sharing, exchanging best practices and benchmarking. The DPO also continued to facilitate relations between the Office and the DPB, fostering effective co-operation in further defining and implementing the EPO data protection framework.

2. Data protection compliance

2.1 Data protection audits

In line with Articles 43(1)(d) and 43(2) DPR, the DPO has been performing data protection audits (DP audits) since 2023 to assist the Office in assessing its compliance with the DPR. DP audits help detect potential irregularities, suggest improvements, mitigate possible risks, and highlight best practices that can be applied across other business areas, in an effort to ensure compliance and continuous improvement.

Figure 2 – DP audits by DG

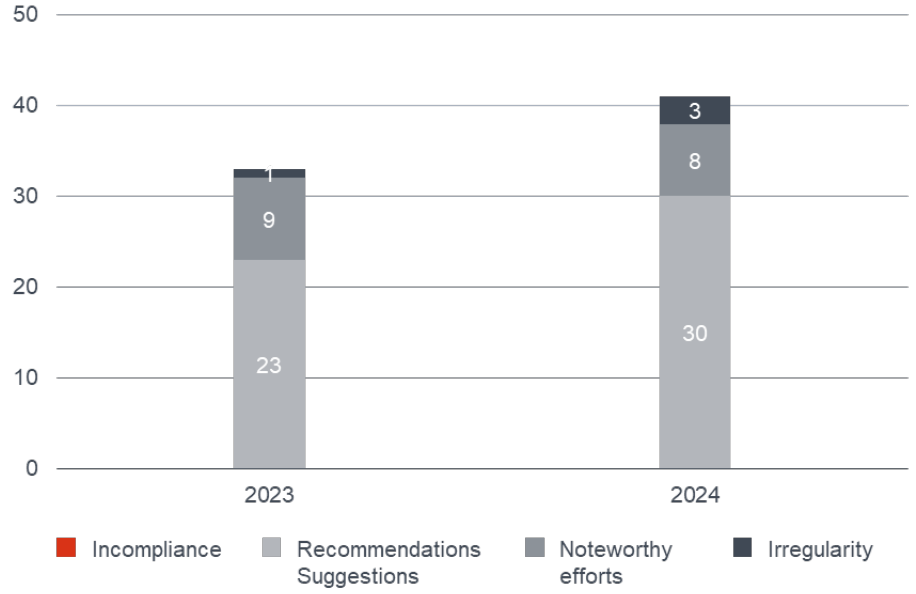


Source: EPO

Data protection audits allow the Office to monitor and improve compliance with the Data Protection Rules.

The audit findings in 2024 showed a good level of compliance overall, with only few irregularities and no incompliances. The DPO provided suggestions for improvement and, in a few cases, commended exemplary practices (noteworthy efforts) put in place by delegated controllers.

Figure 3 – DP audits outcome



Source: EPO

To further enhance the DP audits framework and simplify the process for both DP auditors and auditees, in 2024 the DPO developed a comprehensive list of controls for DP Audits, including controls specifically addressing information security measures and emerging technologies, with the aim of enhancing efficiency and providing even more relevant recommendations.

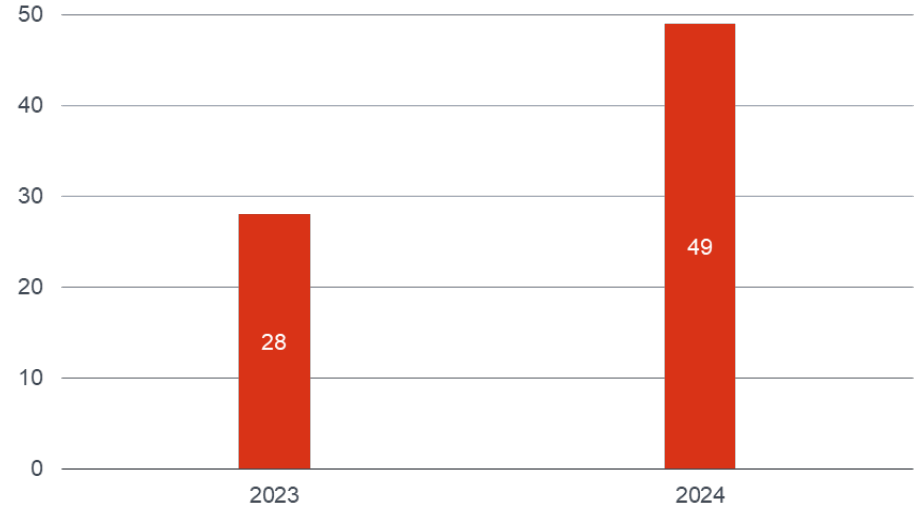
2.2 Risk management

The Office has at its disposal a number of data protection risk management instruments, such as a data protection impact assessment, a transfer impact assessment, and a privacy and security risk assessment.

First launched in 2023, privacy and security risk assessments constitute an important risk management instrument to address and mitigate risks stemming from e.g. outsourcing services and contracts with external parties. They involve several areas of competence, including data protection, legal services and IT security. The number of privacy and security risk assessments conducted by the Office significantly increased in 2024 (+75%).

In an effort towards continuous improvement, all data protection risk assessment instruments were updated and streamlined in 2024.

Figure 4 – Number of privacy and security risk assessments per year



Source: EPO

The growing use of these risk assessment instruments allows the Office to identify and minimise data protection risks by systematically and comprehensively analysing a processing activity and needs to be carried out for any processing that is likely to result in a high risk to individuals.

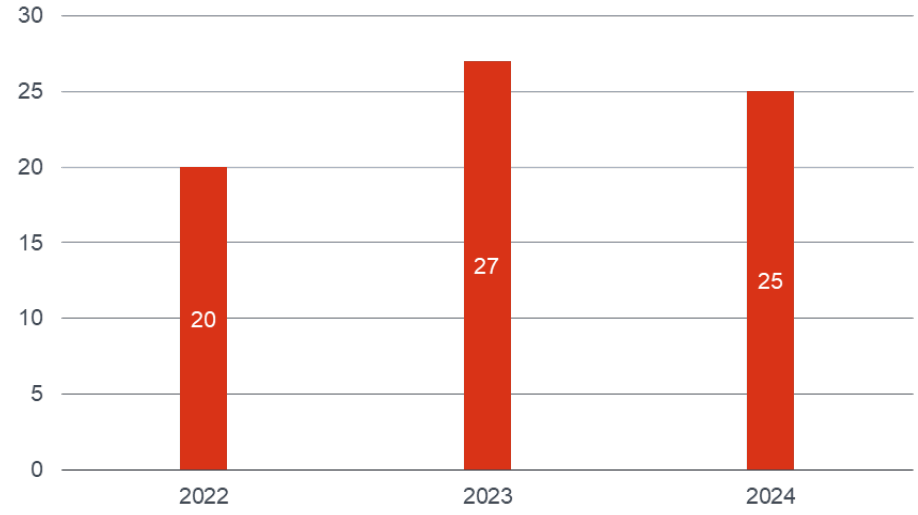
With a view to continuous improvement, risk management procedures were streamlined in 2024, integrating feedback from operational areas and lessons learned from practical use, leading to enhanced efficiency in full respect of the data protection principles.

2.3 Personal data breaches

In accordance with the DPR, the operational units processing the personal data (i.e. delegated controllers) must promptly address any personal data breach and properly assess and mitigate their potentially detrimental effects for individuals. Data breaches are security incidents affecting personal data, e.g. impacting the confidentiality, integrity or availability of the personal data processed by the Office.

The DPO continues to prioritise improving detection and mitigation efforts for personal data breaches.

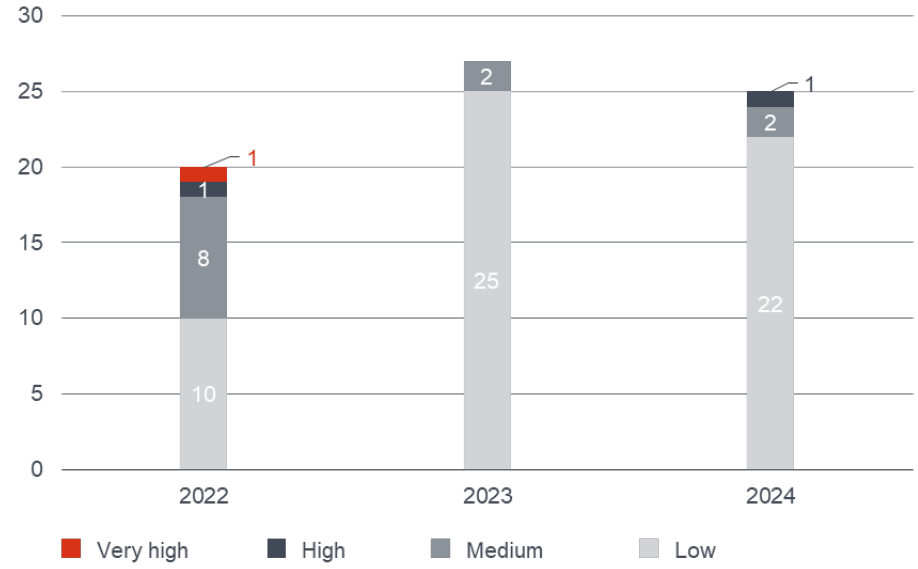
Figure 5 – Detected data breaches per year



Source: EPO

In 2024, the DPO advised delegated controllers on 25 security incidents classified as personal data breaches.

Figure 6 – Number of data breaches by severity



Source: EPO

In the majority of cases (22), the incidents were minor and posed "low" or "no risk" for data subjects. Only two incidents were assessed as "medium risk" and one as "high risk", while none were classified "very high risk". The affected individuals were informed according to the procedure and appropriate mitigating measures aimed, i.a. at avoiding repetition were taken. The Office remains committed to enhancing detection and mitigation efforts of such incidents.

3. Data protection and new technologies

The DPO plays a crucial role in supporting the Office in developing its strategy for integrating new technologies in its operational activities.

The EPO is a leader among international organisations in the integration of new technologies, including AI, while ensuring full compliance with the data protection principles. By leveraging the transformative opportunities offered by AI, the Office aims at increasing efficiency and quality in patent processing and administrative functions. This includes enhancing accuracy, consistency and quality in search and decision-making processes, as well as supporting innovation and sustainability both within the patent systems and beyond.

At the core of this integration is a commitment to respecting and safeguarding fundamental rights and freedoms of individuals. This includes setting standards to ensure legal compliance and ethical decision making, managing data protection risks by safeguarding personal and sensitive information, and employing transparency in AI systems to maintain trust and accountability.

The DPO plays a key role in supporting the Office by analysing and proposing approaches for the integration of new technologies, including AI, promoting the responsible use of AI tools across the Office and ensuring alignment with the Organisation's risk culture, while mitigating potential risks and addressing the impact on the rights and freedoms of data subjects. In 2024, the DPO conducted a comprehensive analysis of AI's impact on data protection rights, developed

criteria for the identification of high-risk AI systems and measures to ensure compliance with data protection requirements. In addition, the DPO organised specialised training sessions on data protection and AI, directed at DPLs and the DPO team to enhance understanding of AI's potential impact and foster expertise on the data protection implications of AI.

Through these actions, the Office ensures that innovation is balanced with robust data protection measures and a commitment to transparency and accountability.

4. Data protection advisory activity

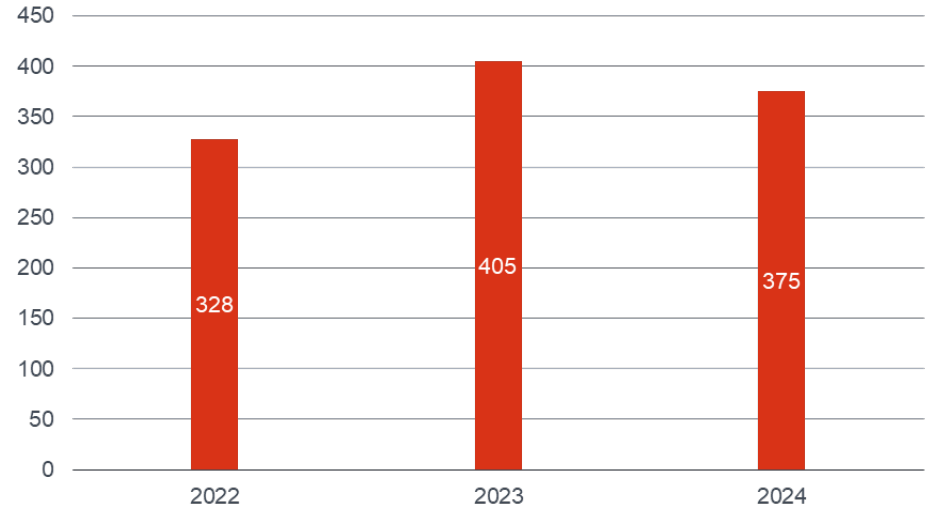
Drawing on the cross-functional expertise of its staff, comprising IT and data protection experts, the DPO provides independent advice on data protection matters to the Office and to data subjects. It also contributes to the strategic projects of the Office by ensuring data protection by design and supports operational units in interpreting the DPR and responding to data subject requests.

The DPO also coordinates the DPLs Network. Each operational unit, i.e. delegated controller, is required to appoint a DPL who serves as the first point of contact for data subject requests, advises delegated controllers on operational data protection issues, performs risk assessments, and conducts awareness-raising activities within their area of competence.

DPLs play a crucial role in implementing the data protection principles at operational level.

In 2024, the DPO provided data protection and technical advice in 375 consultations. While operational requests are dealt with by the DPLs, the DPO continues to be consulted on complex issues regarding the interpretation of the data protection framework and the implementation of operational instruments to ensure transparency and accountability.

Figure 7 – Number of consultations per year



Source: EPO

To continuously enhance the quality of services provided to the Office, the DPO streamlined its internal procedures in 2024. It adopted an internal policy for continuous improvement, revamped its intranet and internet presence to enhance transparency and made all relevant data protection legal and operational instruments accessible to both internal and external stakeholders.

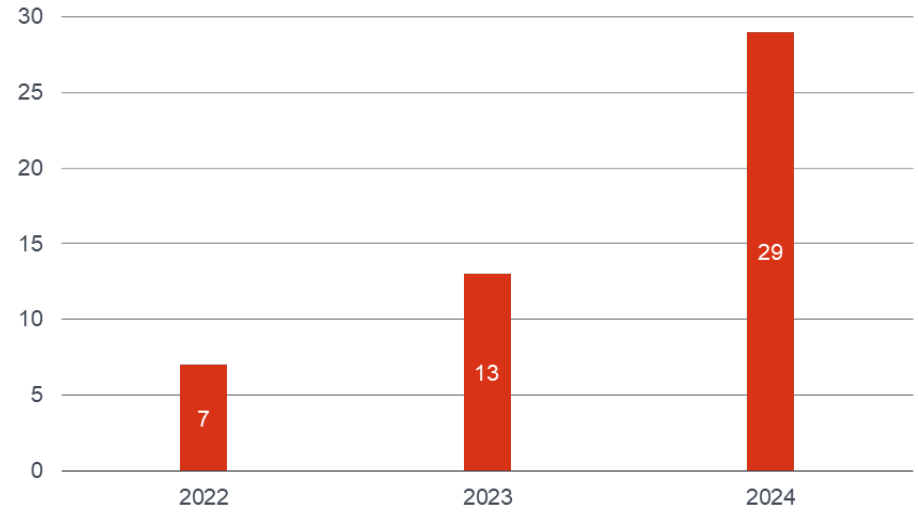
4.1 Data subject requests

The DPO supports delegated controllers in responding to data subject requests to exercise their data protection rights, including right of access, right to object and right to erasure.

Since the DPR entered into force in 2022, the number of data subject requests has steadily increased. In 2024, a total of 29 data subject requests were received, an increase of more than 100% compared to 2023. The majority of these were requests of access to personal data, with 49% coming from external data subjects. A comprehensive procedure for handling data subject requests is in place and tailored training sessions for the DPLs are regularly delivered by the DPO to ensure prompt and adequate response.

The Office has appropriate procedures in place to respond to data subject requests.

Figure 8 – Data subjects requests since entry into force of the DPR



Source: EPO

5. Training and awareness raising

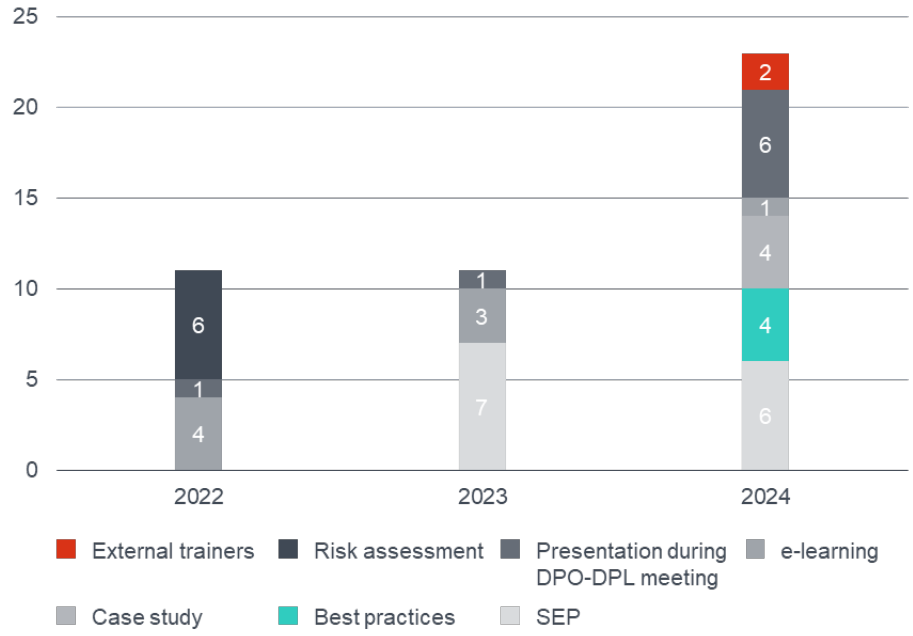
Throughout 2024, the DPO carried out a high number of awareness-raising activities, aimed at further enhancing knowledge of data protection principles and procedures among staff. These include e-learnings, guidance documents, a quarterly DP newsletter ("DPO Highlights"), awareness-raising events on the occasion of Data Protection Day and the Campus Days, specific workshops for managers, and a comprehensive support and enhancement programme for DPLs.

The DPO is continuing its extensive awareness-raising activities with trainings, guidance documents, and e-learning modules.

Many of these activities focused on training DPLs who play a key role in ensuring compliance with the DPR at the operational level and maintaining consistent interpretation and implementation of the DPR across the Office. The DPO has put in place a structured onboarding procedure for new DPLs to equip them with fundamental knowledge of the EPO data protection framework and prepare them for their roles when they join the network. In addition, the DPO provides the DPLs with a specific support and enhancement programme to ensure a consistent interpretation and implementation of the DPR across the Office. The programme comprises general knowledge, ad-hoc sessions on specific issues (data subject requests, data breaches, risk assessments etc.), trainings by external providers,

and analysis of developments in the international data protection landscape, such as judgements by national or international courts or guidance documents by data protection authorities.

Figure 9 – Annual DPL training sessions conducted by the DPO



Source: EPO

6. Co-operation with national patent offices, European institutions and other international organisations

International co-operation in data protection matters is thriving through various initiatives with national patent offices, European institutions and international organisations.

Through the DPO, the Office has further enhanced its co-operation with European institutions and international organisations on issues related to the protection of personal data, working towards an adequacy decision in 2025 as a recognition of the role of the EPO in fostering the highest standards of data protection. In 2024, this collaboration was further enhanced through key initiatives, including the creation of the informal network of DPOs of international organisations. The DPO also actively participated in working groups led by the European Data Protection Supervisor, fostering alignment on data protection practices and strengthening relationships with other international organisations.

Additionally, the DPO engaged in roundtable sessions with national patent offices at TOSC meetings and co-organised an event with the EUIPO to mark Data Protection Day. As a permanent stakeholder in the Corporate Social Responsibility Network, the DPO supported the ongoing development and implementation of the Data Protection as a Corporate Social Responsibility Framework spearheaded by Maastricht University, to further reinforce the Office's commitment to corporate social responsibility, sustainability, transparency and ethical governance. The DPO will continue to actively contribute to these efforts while fostering respect for the fundamental rights and freedoms of individuals.

7. Data Protection Board

The Data Protection Board is an external body with supervisory and advisory functions and is part of the mechanism for legal redress under Article 50 DPR. Together with the DPO, the DPB monitors that the fundamental rights to privacy and data protection are upheld when personal data is processed by the EPO.

To this end, the DPB provides independent, effective and impartial oversight of the application of relevant provisions and examines complaints lodged by current or former staff, as well as external data subjects, regarding data protection issues. Moreover, the DPB issues opinions on the necessity of conducting a data protection impact assessment upon a request from the controller, establishes a list of processing operations that may require a data protection impact assessment and those that do not, and provides consultation and written advice to the controller on various data protection matters.

The DPO continues to foster close and effective collaboration between the Office and the DPB, particularly in areas such as DP audits and inspections, complaint handling, risk assessment instruments and prior consultations. The DPB's guidance remains vital to ensure alignment with other data protection authorities in Europe. In 2024, the DPB dealt with one data subject complaint and issued opinions on different topics. It also adopted its own Code of Conduct, ensuring alignment with the standards of conduct of international civil service as well as the principles and values of the EPO, underlined by the principles of independence, integrity, impartiality, diligence and discretion guiding its activity.