

Data Protection Report 2025

Annex to the Annual Review



Executive summary

Pursuant to Article 43(7) of the Data Protection Rules (DPR), the Data Protection Officer presents an annual report to the President of the EPO, the President of the Boards of Appeal and the Administrative Council. The report provides an overview of the principal activities and accomplishments of the **Data Protection Office (DPO)** during 2025 and indicates its contributions to the Office's broader strategy as enshrined in the Strategic Plan 2028 (SP2028).

In 2025, the EPO reached a milestone in the development of its data protection governance. In an environment marked by rapid technological change, increasing expectations and heightened public scrutiny around the use of personal data, the role of the DPO has continued to evolve from a compliance function to a **strategic enabler of organisational objectives**.

The DPO's activities throughout the year demonstrate that robust data protection is not only a legal requirement but also a **critical component of trust, institutional credibility and sustainable innovation**.

Data protection is deeply embedded in the EPO's strategic priorities. It underpins the Office's ability to operate as a modern, digital-first international organisation, deploy new technologies responsibly and co-operate effectively with European and international partners. The DPO plays a central role in shaping, implementing and safeguarding a data protection framework that supports the EPO's long-term strategy while ensuring a high level of protection for individuals' rights and freedoms.

The highlights of 2025 include:

- **EPO leadership among international organisations:** the **adequacy decision** adopted by the European Commission for the EPO, deeming the EPO data protection framework equivalent to the EU General Data Protection Regulation (GDPR), was a landmark. The EPO is the first international organisation to receive this recognition, confirming the Office's leadership in setting high standards for data protection in the international public sector.
- **Digitalisation and integration of AI:** the DPO plays a central role in supporting the Office's strategic approach to new technologies, with a focus on ensuring data protection compliance in the use of artificial intelligence (AI) in alignment with SP2028 and as part of the DPO AI action plan. This included supporting Business Information Technology (BIT) in drafting the **EPO AI Policy**, issuing **guidance** on data protection and transparent use of AI, and developing a new, integrated **AI impact assessment** as a key instrument for risk management.
- **Partnering with the business:** a key feature of the DPO's work was maintaining a close and continuous partnership with the business areas of the Office. The high number of consultations handled during the year (487, +30% compared with 2024) reflects both the increasing complexity of **data-driven processes** and the trust placed in the **DPO** as a **strategic advisor**. The DPO provided guidance on a broad spectrum of topics, including the interpreting and applying the DPR, handling data subject requests and managing personal data breaches. This hands-on support enabled operational units to make informed decisions, mitigate risks at an early stage and integrate data protection considerations seamlessly into their daily

activities. By fostering a solution-oriented dialogue, the DPO helped translate legal requirements into practical and proportionate measures that support the Office's operational effectiveness.

- **Monitoring compliance and oversight:** compliance remained at the heart of the DPO's mandate. The DPO continued to monitor the application of the DPR, oversee corrective actions where necessary and **promote accountability** across the organisation. Through structured oversight, documentation and reporting, the DPO ensured that data protection compliance is demonstrable, measurable and continuously improved.
- **Raising awareness and promoting a culture of data protection:** this remains a core pillar of the DPO's strategy. Recognising that compliance depends not only on rules and procedures but also on people, the DPO continued to invest in building a strong **data protection culture across the Office**. Targeted training sessions, tailored guidance materials and regular communication initiatives were delivered to address the specific needs of different staff groups. Emphasis was placed on emerging topics such as AI and the secure handling of sensitive data.
- **Co-operation and institutional engagement:** co-operation with external partners was further enhanced. Having founded a **network of DPOs of international organisations** in 2024, which now brings together 30 organisations, the DPO built on this key platform for exchanging best practices and addressing common challenges. **Co-operation with European institutions** – including the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) – also expanded, notably through several initiatives related to AI. In parallel, the DPO continued to play a central role in reinforcing co-operation between the Office and the **Data Protection Board (DPB)**, supporting the further development and effective implementation of the EPO data protection framework.

The activities outlined in this report illustrate how the DPO's actions contribute directly to the EPO's strategic objectives. While challenges remain, by combining legal rigour, operational support and strategic foresight, the DPO helps ensure that data protection remains a source of trust, resilience and competitive advantage for the Office in an increasingly data-driven world.

Contents

Executive summary	2
1. DPO advisory activity in support of the business	5
1.1 Data subject requests	6
2. Data protection compliance and oversight	6
2.1 Data protection audits	6
2.2 Personal data breaches	7
3. Risk management	9
4. Data protection and AI	9
4.1 Safeguarding fundamental rights while deploying AI	10
4.2 The DPO as a knowledge hub for AI	10
5. Strengthening a culture of data protection	11
5.1 The DPL network	11
6. Adequacy decision	12
7. Co-operation with European institutions, NPOs and international organisations	13
8. Co-operation with the Data Protection Board	14
9. Remaining challenges and strategic outlook	14

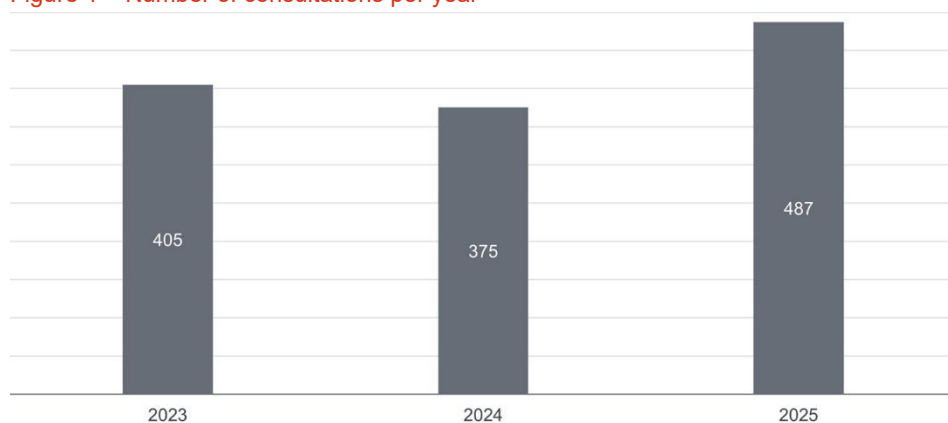
1. DPO advisory activity in support of the business

One of the main activities carried out by the DPO consists in the provision of comprehensive legal and technical guidance on data protection matters across the Office. This includes support to the Boards of Appeal, the Administrative Council, delegated controllers, and data subjects. The DPO also plays an active role in strategic Office initiatives, ensuring data protection is integrated by design in projects, and assists operational units with interpreting the DPR and handling delicate cases, such as data subject requests.

The DPO was involved in **487 consultation cases** in 2025. This represents a significant increase compared to the previous year (**+30%**), underscoring both the growing complexity of the Office's data protection landscape and the continued reliance on the DPO's expertise.

The rising volume of consultations highlights the DPO's active engagement across the organisation and reflects the increasing necessity for expert advice and guidance, particularly in the context of new initiatives, technology adoption, and evolving data protection needs within the Office's operational landscape.

Figure 1 – Number of consultations per year



Source: EPO

A large proportion of the consultations related to ensuring compliance with the DPR. Last year saw a notable increase in IT-related inquiries involving technical aspects of IT systems and services, which accounted for 69 consultations, or 15% of the total. This was followed by a rise in HR-related issues (63 consultations, 14%), legal matters (51 consultations, 12%), core business areas (DG1 and BoA) (31 consultations, 7%), and communications (24 consultations, 5%).

The DPO also participated in a range of collaborative projects with other units across the Office, ensuring that the rights and freedoms of data subjects are adequately protected.

1.1 Data subject requests

The DPR provide data subjects with several rights with regard to the processing of their personal data. These include the right to of access, the right to object, the right to rectification, and the right to erasure (commonly known as the "right to be forgotten"). The DPO supports the delegated controllers in assessing these requests and providing the necessary replies, as appropriate.

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

25 data subject requests were received in 2025, either directly by the DPO or via organisational units seeking expert advice. The majority of requests concerned **access to personal data**, with **44% submitted by external data subjects**.

Data subject requests were managed effectively thanks to the DPO's proactive measures, including implementation of a comprehensive workflow for handling requests and provision of targeted training sessions for Data Protection Liaisons (DPLs), ensuring timely and high-quality responses.

2. Data protection compliance and oversight

2.1 Data protection audits

Back in 2023 the DPO further deepened its oversight role by starting to carry out **data protection audits (DP audits)**. The aim is to support the Office in evaluating compliance with the DPR. DP audits are a precious tool to identify potential weaknesses in the Office's operations, recommend improvements, mitigate risks, and promote best practices and noteworthy efforts across business areas, safeguarding transparency and accountability to data subjects.

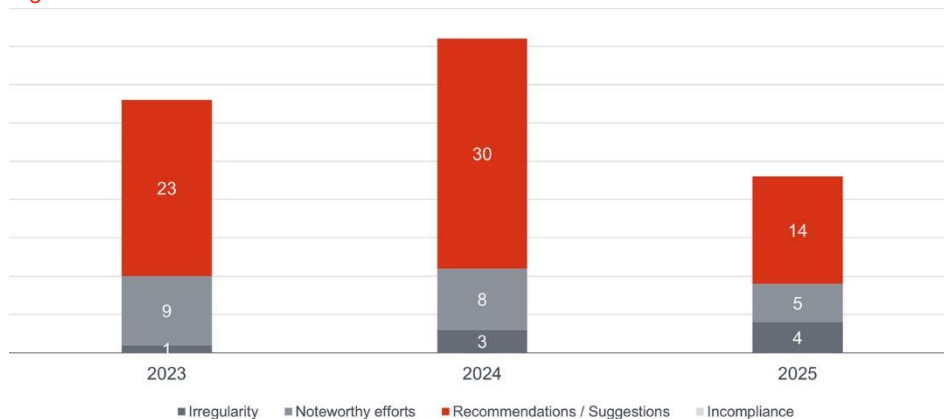
In accordance with the Annual DP Audit Plan, in 2025 the DPO carried out four audits across various organisational units. Following the DP audit methodology, the DP audits aimed to (i) evaluate the lawfulness of data processing activities, (ii) assess the efficiency of existing controls and processes, (iii) validate readiness for incident responses and data breaches, and (iv) identify areas of incompliance and ensure these remedied.

Data protection audits allow the Office to monitor and improve compliance with the DPR

The result of the DP audits carried out in 2025 indicated a generally high level of compliance across the Office. Minor irregularities were detected, such as inconsistencies within certain data protection documentation. **No cases of incompliance** were identified.

In accordance with the DP audit methodology, the DPO issued targeted recommendations and suggestions for improvement and highlighted commendable practices. Overall, the results confirmed the continuous commitment of the audited units to integrating data protection principles into their daily operational work.

Figure 2 – Outcome of DP audits



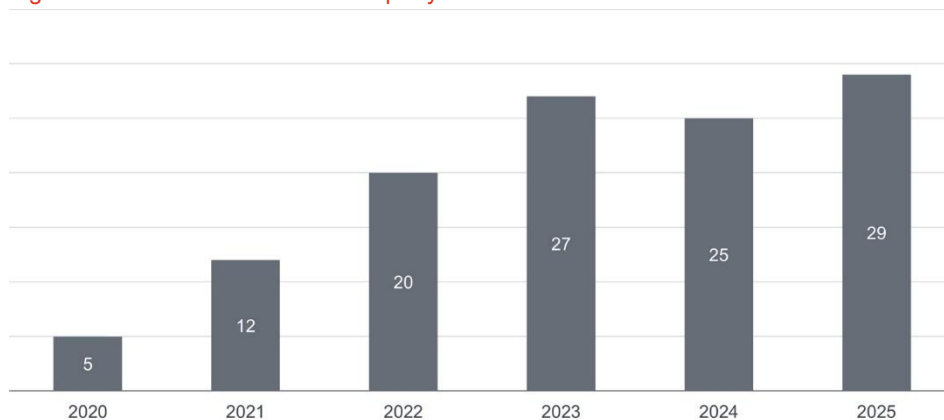
Source: EPO

2.2 Personal data breaches

Article 34 DPR requires delegated controllers to react swiftly to any security incident potentially constituting a personal data breach and evaluate and mitigate potentially adverse consequences. The DPR mandate that all personal data breaches must be reported to the DPO without undue delay and, depending on the risk to their rights and freedoms, the individuals involved must be informed of the breach. 29 security incidents identified as personal data breaches were reported to the DPO in 2025.

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

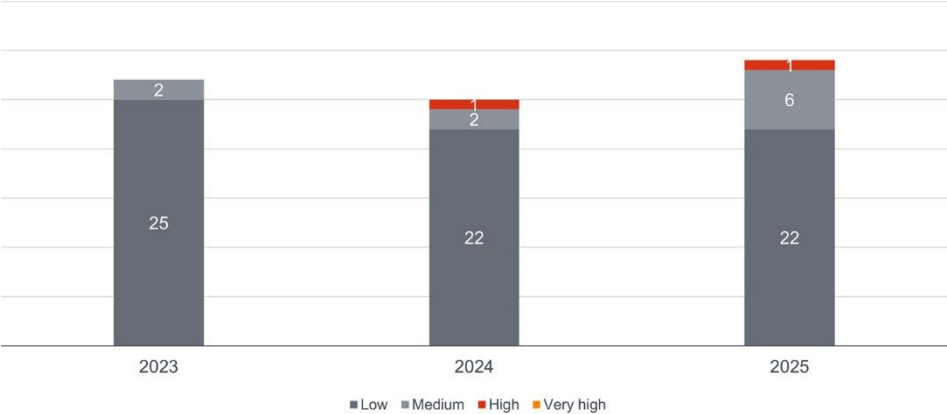
Figure 3 – Detected data breaches per year



Source: EPO

Most of the incidents assessed by the delegated controller with the assistance of the DPO were concluded as posing "low" or "no risk" to the individuals concerned. Only six were evaluated as "medium risk", and one as "high risk"; none reached the "very high risk" category.

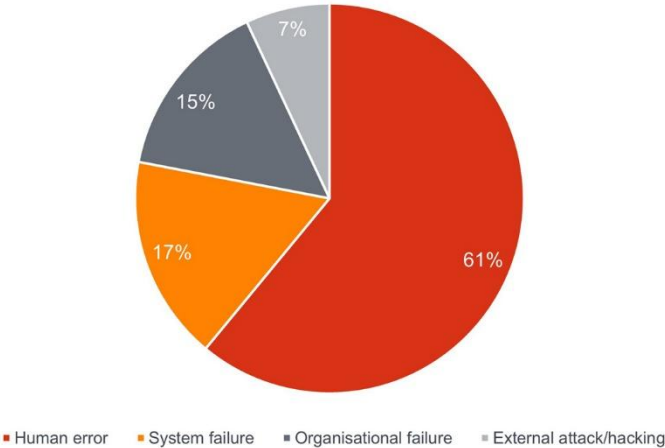
Figure 4 – Number of data breaches by severity



Source: EPO

Given that personal data breaches may lead to physical, material or non-material damage to individuals, data controllers must continuously monitor such incidents, assess their causes, evaluate the risks based on the potentially adverse effects on the rights and freedoms of the data subject and implement appropriate mitigating measures. To support this, the DPO analysed the personal data breaches reported between 2022 and 2024, classifying them by root cause and suggesting targeted measures. The analysis revealed that the main cause was human error (43 breaches), followed by system failure (12 breaches), organisational failure (11 breaches) and external attacks/hacking (5 breaches). Most breaches attributed to human error stemmed from misdirected emails and inadequate access rights management.

Figure 5 – Personal data breaches by category



Source: EPO

3. Risk management

The DPO is a key driver of risk mitigation in the organisation, safeguarding against legal, financial and reputational exposure. Through proactive oversight and advice, the DPO turns data protection compliance into a risk management advantage and actively promotes a positive vision and collective commitment to privacy and data protection, ensuring understanding of and compliance with the relevant roles and responsibilities and the principle of accountability.

Since DPR came into force the DPO has developed a comprehensive approach for managing data protection risks, incorporating methodologies and templates for carrying out **data protection impact assessments** (DPIAs), **transfer impact assessments** (TIAs) and **privacy and security risk assessments** (PSRAs).

To further streamline the Office's data protection instruments, in 2025 the DPO developed and published a revised TIA methodology which offers clearer guidance and a more pragmatic approach, enhancing the operational effectiveness of TIAs and supporting delegated controllers in better assessing and managing the risks related to cross-border personal data transfers.

As DPIAs are currently the most effective tool for assessing risks linked to new technologies, they are also the starting point for understanding how AI may impact data protection at the Office. Following the AI Policy, DPO developed an **integrated data protection and AI impact assessment** which strengthens the Office's ability to manage emerging technological risks proactively. This approach ensures that privacy, ethical and legal considerations are embedded from the earliest stages of developing and deploying AI, reducing the likelihood of compliance breaches, bias or reputational damage. The integration of these assessments also enables a holistic view of data and AI-related risks, providing senior management with actionable insights to make informed, risk-aware decisions that support the long-term business objectives.

In an effort towards continuous improvement, all data protection risk assessment instruments were updated and streamlined in 2025

4. Data protection and AI

The responsible integration of new technologies, in particular AI, is a cornerstone of SP2028. In 2025 the DPO continued to play a central role in supporting this strategic ambition by ensuring innovation is accompanied from the outset by strong protection for the rights and freedoms of individuals.

By implementing a Data Protection and AI Action Plan the DPO provided structured and forward-looking support to AI-related initiatives across the Office. This included early involvement in project design, guidance on data minimisation, transparency, and fairness, and the assessment of risks to individuals through tailored DPIAs.

Embedding data protection by design and by default into AI use cases allows the DPO to actively contribute to building trust in new technologies and enabling lawful and ethical deployment of them.

This proactive approach ensures the Office can leverage the benefits of AI while remaining fully aligned with evolving regulatory and ethical expectations at European and international level.

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

4.1 Safeguarding fundamental rights while deploying AI

Leveraging the potential of AI is key for the operational efficiency and quality of services of the Office, offering the opportunity for gains in precision, consistency and quality in decision-making processes, alongside broader support for sustainability and innovation both within the patent system and in related domains.

This evolution must be guided by a strong dedication to protecting fundamental rights and individual freedoms.

Core priorities for the DPO include:

- Managing data protection risks, especially when handling sensitive personal data.
- Ensuring transparency to foster trust and uphold accountability in the deployment of AI tools.

The DPO aims to ensure focused, transparent use of AI and strengthen trust, data protection, and responsibility across the organisation

4.2 The DPO as a knowledge hub for AI

As part of its commitment to continuous improvement and maintaining the EPO's leadership position among international organisations, the DPO acts as a knowledge hub for emerging technologies, with a particular focus on AI and its implications for data governance.

The DPO closely monitors global regulatory, technological and ethical developments in the field and systematically assesses their implications for data protection, fundamental rights and organisational accountability.

In 2025 the DPO undertook a comprehensive set of initiatives aimed at enabling **responsible, transparent and compliant integration of AI systems** within the Office.

These actions were designed to ensure innovation is pursued in full alignment with data protection principles, strengthening the Office's data governance framework and supporting its strategic digital transformation objectives.

Key contributions during the year included:

- Supporting the Office in the drafting of the **EPO Policy on the Use of Artificial Intelligence Systems**, ensuring it reflects data protection by design and by default.
- Being the first international organisation to design an **integrated AI impact assessment framework** for high-risk AI systems under the AI Policy, consolidating data protection, ethical and fundamental rights considerations into a single coherent tool.
- Producing data protection **guidelines and instruments** to address AI-specific risks and safeguards.
- Contributing to internal and external communication activities on the processing of personal data in AI, including organising a **joint event with other international organisations** dedicated to AI and data protection.
- Integrating AI risk identification and assessment components into the support and enhancement training programme for **DPLs**, strengthening local expertise across the organisation.

Through these actions the DPO contributed to **establishing a safe, trustworthy and future-proof digital ecosystem** at the EPO. By strengthening the balance between protection, accountability and innovation the DPO supports the development of secure and interoperable systems that safeguard individuals' rights while enabling responsible, transparent and evidence-based use of data. This approach not only enhances operational efficiency, it also reinforces **trust and institutional credibility**.

Looking ahead, 2026 will be marked by a further consolidation of this work through close and structured collaboration with key stakeholders, including BIT, Legal and PD People. Joint efforts will focus on strengthening data governance structures, refining accountability mechanisms and supporting the safe and compliant integration of emerging technologies, ensuring the EPO remains at the forefront of responsible digital innovation.

5. Strengthening a culture of data protection

The DPO conducted a wide range of **awareness-raising activities** in 2025 aimed at strengthening data protection culture across the Office. These included developing and rolling out **e-learning modules** on data protection in the patent granting process and on procurement, as well as various **guidance** documents and other communication measures, including an event on AI organised on **Data Protection Day** in collaboration with other international organisations (CERN, EMBL, the ESA and the ESO).

A significant share of these initiatives focused on supporting the DPLs, with targeted training on key data protection topics, and ad hoc briefings on complex or emerging issues to ensure uniform interpretation and application of the DPR.

5.1 The DPL network

Responsibility for coordinating the network of DPLs lies with the DPO. For the purpose of assistance in data protection matters (e.g. data subject requests, risk assessments and awareness-raising exercises) each delegated controller must appoint a DPL.

DPLs play a central role in the data protection framework by supporting delegated controllers and business units in applying data protection principles and conducting first-level monitoring of processing operations. The role of the DPLs has been enhanced by several measures aimed at stabilising their number, increasing their knowledge and enhancing their efficiency and effectiveness in the data protection framework.

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

The EU adequacy decision makes the EPO the first international organisation with GDPR-level protection, boosting trust, co-operation, efficiency and ease of data transfers

6. Adequacy decision

2025 marked a landmark year for the DPO and the Office as a whole; the European Commission formally adopted the **adequacy decision** for the EPO, recognising that the Office provides a level of protection to personal data that is equivalent to that guaranteed under EU law in the GDPR. This is a historic milestone. The EPO stands as the first international organisation to receive such recognition.

The EPO issued an adequacy decision on the EU in 2022. The Commission adequacy decision completes the process of mutual recognition of privacy standards. This will allow EU institutions, Member States, public authorities and private entities in the EEA to transfer personal data directly to the EPO without the need for additional safeguards, streamlining international co-operation, improving operational efficiency and fostering innovation.

The adequacy decision is the result of sustained efforts over several years to develop, implement and continuously improve a comprehensive and coherent data protection framework. It represents a significant achievement for the DPO and underscores the Office's continued commitment to the highest standards of data protection and transparency.

Key benefits for the Office of the adequacy decision include:

- **Reputational excellence:** being the first international organisation ever to receive an EU adequacy decision demonstrates the leading role the EPO plays in data protection and sets a benchmark for compliance and best practices. This milestone enhances the Office's credibility and visibility as a trustworthy and responsible data controller.
- **Improved international co-operation:** the adequacy decision facilitates seamless data transfers with national patent offices (NPOs) of EU Member States, removing legal and administrative barriers under the GDPR. It supports the development of new partnerships and reinforces existing collaborations through mutual trust. It has also allowed the DPO, as the Office's data protection authority (DPA), to join the European Data Protection Board (EDPB) group of DPAs from countries with an EU adequacy decision, giving the EPO an unprecedented platform to help shaping data protection policy-making at the international level, while providing the unique point of view of an international organisation.
- **Contractual advantages:** the adequacy decision makes it easier to negotiate data-sharing agreements with EU private entities and establishes a pre-defined, EU-scrutinised framework for transferring personal data to the EPO without the need for specific contractual clauses under the GDPR or TIAs.
- **Operational efficiency:** the adequacy decision enables the Office to accelerate exchanges of personal data, improving decision-making speed and operational responsiveness while saving resources, especially in high-volume and time-sensitive projects. It reduces administrative burden by removing the need to assess and implement additional safeguards for each data transfer under the GDPR.

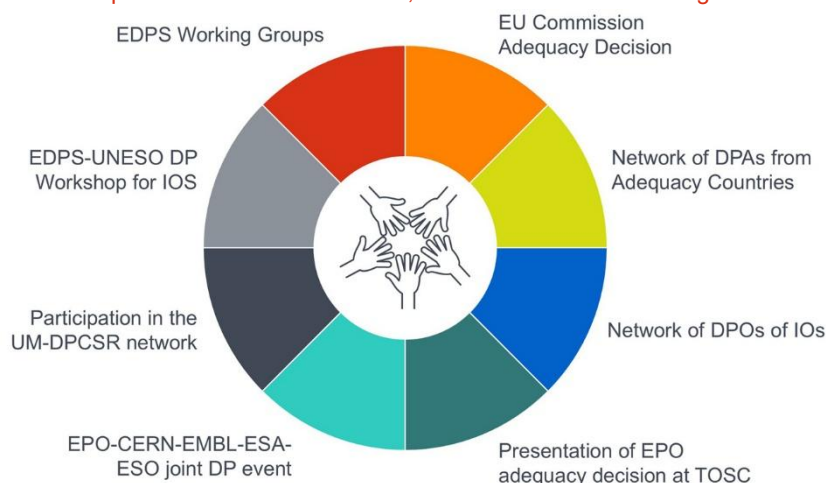
7. Co-operation with European institutions, NPOs and international organisations

The DPO continues to engage actively with European institutions, NPOs and international organisations. In 2025 this co-operation was further strengthened through several initiatives, notably the adequacy decision by the **European Commission** and the enlargement of the informal **network of DPOs of international organisations**, which now brings together 30 such bodies. To support the network's growing scope and foster more structured collaboration, a steering committee was established. Its inaugural meeting took place in December, bringing together several international organisations that volunteered to contribute to shaping effective and trusted co-operation among DPOs.

The DPO also joined in roundtable discussions with NPOs at **TOSC** meetings and co-organised a **joint event**, "AI beyond the hype – Challenges and opportunities for data protection" in conjunction with CERN, EMBL, the ESA and the ESO to celebrate Data Protection Day. As a standing member of the **Corporate Social Responsibility Stakeholders Group**, the DPO joined the Working Group of International Organisations to analyse the how the framework applies to international organisations and explore how it might be adapted.

International co-operation in data protection matters is thriving, with various initiatives between NPOs, European institutions and international organisations

Figure 6 – Co-operation with EU institutions, NPOs and international organisations



Source: EPO

The DPO participated in the annual **Data Protection Workshop for International Organisations** co-hosted by the European Data Protection Supervisor (EDPS) and UNESCO as a panellist on "Recent developments and practices for international transfers to and between international organisations". Having represented the Office since 2021, the DPO shared insights into the process that led up to the adequacy decision and further reinforced the EPO's leadership role among international organisations in the field of data protection in the wake of that decision.

For the first time the DPO participated in the **network of DPAs from countries with an EU adequacy decision (adequacy countries)** launched by the EDPB to facilitate exchanges and co-operation opportunities. The main topics of discussion were AI and data protection, online tracking, child data protection and international data protection enforcement co-operation.

Participation in these various networks offers the Office valuable visibility into the current priorities of regulators and the direction of upcoming developments, enabling it to anticipate changes and adjust its strategies accordingly. The Office presence provides an opportunity to contribute to the development of emerging standards and best practices.

8. Co-operation with the Data Protection Board

The DPO continued to cultivate the relationship between the DPB and the EPO, acting as a central link and fostering effective co-operation. Regular meetings allowed alignment on the key projects and initiatives of the DPO and one in-person session was organised.

The DPB handled its second **data subject complaint** in 2025. Building on experience gained from the first Article 50 case in 2024, and in consultation with the DPB, the DPO revised the DPB's internal workflows in line with its Rules of Procedure. The revisions aimed to align procedures with updated Office systems and tools, clarify deadlines, streamline the complaint process and ensure timely legal certainty for data subjects. The DPB also issued an opinion on assessing damages and awarding compensation for data protection infringements. This guidance clarifies the conditions under which data subjects may claim damages and the factors to consider in determining the level of compensation. It also promotes consistent handling of such claims across the Office's bodies and stakeholders.

9. Remaining challenges and strategic outlook

While 2025 marked significant progress in the maturity of the EPO's data protection framework, several structural and strategic challenges remain. Addressing these will be crucial to sustaining compliance, preserving institutional trust and enabling the Office's continued digital transformation in an increasingly complex international environment.

At organisational level, the accelerating adoption of **data-driven technologies** – particularly AI systems and AI components in tools in use at the Office – continues to challenge traditional governance and risk management models. **Ensuring that data protection, data governance and accountability** mechanisms scale effectively with technological innovation requires early and systematic involvement of the DPO in strategic initiatives, as well as clear ownership of data-related risks across the organisation. Embedding data protection by design and by default into complex, multi-stakeholder projects remains a key priority and requires sustained commitment at senior management level.

The **growing volume and complexity of personal data processing activities** also place increasing demands on operational units. High expectations for responsiveness, transparency and compliance, particularly in relation to data subject rights and incident management, necessitate further investment in processes, tools and skills. Strengthening decentralised capabilities while maintaining consistent central oversight remains a delicate balance that the DPO will continue to address through guidance, training and targeted support.

From a **broader international perspective**, the regulatory and policy landscape is evolving rapidly. Emerging approaches to data protection, AI and digital governance across jurisdictions are creating increasing complexity. While the adequacy decision confirms the robustness of the EPO's framework, maintaining this level of equivalence over time will require continuous adaptation, close monitoring of regulatory developments and proactive engagement with European and international partners.

At the same time, the expectations placed on international organisations are rising. Stakeholders increasingly look to institutions such as the EPO to demonstrate leadership not only in compliance, but also in **ethical, transparent and accountable use of data**. This reinforces the need for the DPO to continue evolving as a strategic advisor, bridging legal requirements, technological innovation and organisational governance.

Looking ahead, the DPO's ability to address these challenges will depend on sustained senior-level sponsorship, strong cross-departmental co-operation and the integration of data protection and data governance considerations into strategic decision-making. If it succeeds in reinforcing these foundations, the Office will be well positioned to navigate future risks, leverage innovation responsibly and maintain its role as a trusted and forward-looking international organisation.