



EUROPEAN DATA PROTECTION SUPERVISOR

Annual Activity Report

2022

Contents

1.	Introduction	6
2.	Operational achievements	7
2.1	The EDPS in 2022	7
2.1.1.	EDPS Conference 2022	7
2.1.2.	Data Protection in a global health crisis	7
2.1.3.	Leading by example in safeguarding EU digital rights	8
2.1.4.	Shaping a safer digital future for the EU	24
2.1.5.	The EDPS as a member of the EDPB.....	31
2.1.6.	International cooperation in data protection	33
2.2	The EDPB in 2022	36
2.2.1.	EDPB 2022 Highlights	36
2.2.2.	Meetings.....	40
2.2.3.	Guidelines, Opinions, Decisions and other documents.....	41
2.2.4.	Stakeholder engagement	50
2.2.5.	The EDPB Secretariat contribution to the national SAs' cooperation	50
2.2.6.	IT communications tool (Internal Market Information) & the new EDPB website	51
2.2.7.	The EDPB Secretariat activities relating to access to documents	52
2.2.8.	The EDPB Secretariat activities relating to Data Protection Officer activities	52
2.2.9.	Coordinated Supervision Committee (CSC).....	53
3.	Resource management	55
3.1.	The EDPS Ethics Framework Activities.....	55
3.2	Human resources.....	57
3.2.1	Staff working conditions and wellbeing.....	57
3.2.2	Careers: From recruiting data protection experts to exit interviews.....	57
3.2.3	Evolving organisation	59
3.3	Budget	59
3.3.1.	Allocated budget for 2022	59
3.3.2.	Budget execution 2022	59
3.3.3	Working methods	60
3.3.4	Draft budget 2023 exercise.....	60
3.3.5.	Discharge 2020 Budget	61
3.3.6	Staff.....	61
3.4	Procurement and contracting.....	62
3.4.1	Professionalization	62
3.4.2	Framework contracts and concluded contracts.....	62
3.5.	Finance	63
3.6	Missions management.....	64
4.	Management and internal control	65
4.1	Characteristics and nature of activities	65
4.1.1	The mission of the EDPS.....	65
4.1.2	Core values and guiding principles.....	67
4.1.3	Data Protection and the EDPS in 2022.....	67
4.2	Strategy 2020-2024	69
4.2.1	EDPS strategic objectives	69
4.2.2	Action plan	69
4.2.3	Measuring performance	69
4.3	Inter-institutional cooperation	70
4.4	Ex-post controls	71
4.5	Events during the year that affected reputation	71
4.6	Internal control management system	71
4.7	Internal evaluation of the internal control system and indicators underpinning the statement of assurance.....	72
4.8	Cost effectiveness and efficiency of Internal Control.....	73
4.9	Results of independent audit during the year	73
4.9.1	Court of Auditors.....	73

4.9.2 Internal Audit Service (IAS)	74
4.9.3 Internal Control Standards (ICS) monitoring situation.....	75
4.9.4 Discharge procedure	76
4.10 Conclusions on the effectiveness of internal control	76
5. Reservations and impact on the statement	76
5.1 Materiality criteria.....	76
5.1.1. Objectives of materiality criteria.....	77
5.1.2. Qualitative criteria.....	77
5.1.3. Quantitative criteria	77
5.1.4. Criteria of the Internal Audit Service.....	77
5.2 Reservations	77
5.3 Conclusion	77
6. Statement of assurance from the authorising officer by delegation.....	78
7. Annexes	79
Annex 1: Summary of annual activity report	79
Annex 2: Human resources at the EDPS	80
Annex 3: Budget 2022	82
Annex 4: Detailed list of missions undertaken by the Supervisor (2022)	85
Annex 5: EDPS strategic objectives	86
Annex 6: EDPS strategic objectives and its Action Plan	87

List of acronyms

AA	Administrative Arrangement
AAR	Annual Activity Report
ABAC	Accrual Based Accounting System
AFSJ	Area of Freedom Security and Justice
AI	Artificial Intelligence
AMP	Annual Management Plan
AOD	Authorising officer by delegation
APC	Audit Progress Committee
BCR	Binding Corporate Rules
CATE	Case Analysis Tool Environment
CICED	Core International Crimes Evidence Database
CIS	Customs Information System
CEF	Coordinated Enforcement Framework
CMS:	Case Management System
CSAM	Child Sexual Abuse Material
CSC	Coordinated Supervision Committee
DG	Directorate-General
DPA	Data Protection Authority
DPbDD	data protection <i>by design</i> and <i>default</i>
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EASO	European Asylum Support Office
EC	European Commission
ECB	European Central Bank
ECA	European Court of Auditors
ECRIS-TCN	European Criminal Records Information System on non EU-nationals
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EES	Entry/Exit System
EIB	European Investment Bank
EP	European Parliament
EPPO	European Public Prosecutors' Office
EPSO	European Personnel Selection Office
ETIAS	European Travel Information and Authorisation System
EUCI	EU Classified information
EUDPR	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data
EUIs	European institutions, bodies, offices and agencies
euLISA	European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
EURODAC	European Asylum Dactyloscopy Database
Eurojust	European Union Agency for Criminal Justice Cooperation

Europol	European Union Agency for Law Enforcement Cooperation
EUSA	European School of Administration
Frontex	European Border and Coast Guard Agency
FTE	full time equivalent
GDPR	' General Data Protection Regulation ' Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
GPA	Global Privacy Assembly
HRBA	Human Resources and Budget Administration
IAS	European Commission Internal Audit Service
ICC	Internal Control Coordinator
ICS	Internal control standards
IMI	Internal Market Information
IPEN	Internet Privacy Engineering Network
KPI	key performance indicator
LSA	Lead Supervisory Authority
MFF	Multiannual Financial Framework
NGO	Non-governmental organisation
OECD	Organisation for Economic Co-operation and Development
OSS	One stop shop
PMO	Paymaster Office of the European Commission
SA	Supervisory Authority
SIAP	Strategic Internal Audit Plan
SIS	Schengen Information System
SLA	Service Level Agreement
SoA	Statement of Assurance
SPE	Support Pool of Experts
VIS	Visa Information System

1. Introduction

The Financial Regulation (Article 74.9¹) stipulates that each **authorising officer by delegation** (AOD) shall submit an annual activity report to their Union institution, together with financial and management information. This report shall present the achievements of their institution in relation to the resources used. It shall also be a management report on performance in the context of their task as AOD. This requirement is the logical consequence of paragraph 2² of this same article, which gives the AOD responsibility for internal controls.

In the annual activity report of the AOD, this latter must include a statement of assurance (“Statement”) based on their own judgment and on the information available in which the AOD:

- states that the information contained in the report gives a true and fair view;
- declares that the AOD has reasonable assurance that the resources allocated to the activities described in the report have been used for their intended purposes and in accordance with principles of sound financial management, and that the control procedures put in place give the necessary guarantees as to the legality and regularity of the underlying transactions;
- confirms that the AOD is not aware of any matter not reported which could harm the interests of the institution.

¹ Financial Regulation, Article 74(9): The authorising officer by delegation shall report to his or her Union institution on the performance of his or her duties in the form of an annual activity report containing financial and management information, including the results of controls, declaring that, except as otherwise specified in any reservations related to defined areas of revenue and expenditure, he or she has reasonable assurance that:

- (a) the information contained in the report presents a true and fair view;
- (b) the resources assigned to the activities described in the report have been used for their intended purpose and in accordance with the principle of sound financial management; and
- (c) the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

The annual activity report shall include information on the operations carried out, by reference to the objectives and performance considerations set in the strategic plans, the risks associated with those operations, the use made of the resources provided and the efficiency and effectiveness of internal control systems. The report shall include an overall assessment of the costs and benefits of controls and information on the extent to which the operational expenditure authorised contributes to the achievement of strategic objectives of the Union and generates EU added value. The Commission shall prepare a summary of the annual activity reports for the preceding year.

The annual activity reports for the financial year of the authorising officers and, where applicable, authorising officers by delegation of Union institutions, Union bodies, European offices and agencies shall be published by 1 July of the following financial year on the website of the respective Union institution, Union body, European office or agency in an easily accessible way, subject to duly justified confidentiality and security considerations.

² Financial Regulation, Article 74(2): For the purposes of paragraph 1 of this Article, the authorising officer by delegation shall, in accordance with Article 36 and the minimum standards adopted by each Union institution and having due regard to the risks associated with the management environment and the nature of the actions financed, put in place the organisational structure and the internal control systems suited to the performance of his or her duties. The establishment of such structure and systems shall be supported by a comprehensive risk analysis, which takes into account their cost effectiveness and performance considerations.

2. Operational achievements

2.1 The EDPS in 2022

The EDPS' [Strategy for 2020-2024](#) overarching aim is to shape a safer digital future, with three core pillars outlining the guiding actions and objectives for the organisation to the end of 2024: **Foresight, Action and Solidarity**. These three pillars, and our strategy as a whole, were the driving force for our work in 2022.

2.1.1. EDPS Conference 2022

The idea of hosting a conference by the European Data Protection Supervisor (EDPS) was born out of the EDPS 2020-2024 Strategy, where the wheels were set in motion for the EDPS to host a conference discussing how to safeguard effectively individuals' rights to privacy and data protection, as enshrined in the European Union Charter of Fundamental Rights.

With this conference, the EDPS planned to create a platform to bring the world's best practices together, and steer meaningful discussions about the digital regulatory sphere, seeking to acknowledge that there is scope for discussions on potential improvements of the enforcement of data protection rules. On 16 & 17 June 2022, this conference became a reality. Entitled "The Future of Data Protection: Effective Enforcement in the Digital World", the conference brought together over 2 000 participants, both in Brussels and online. Featuring over one-hundred speakers; three main sessions; sixteen breakout sessions; nine individual keynote remarks; and five side events, the two-day event fostered crucial conversations on the future of data protection, with a particular focus on the enforcement of the General Data Protection Regulation (GDPR).

2.1.2. Data Protection in a global health crisis

Following the outbreak of the COVID-19 pandemic, the EDPS immediately established an internal [task force](#) to actively monitor and assess both the EU's and EU Institutions (EUIs) responses to the outbreak.

Throughout 2021 and the first part of 2022 (until the slow-down of the pandemic), the COVID-19 task force continued following developments and preparing for the future of data protection and privacy after the COVID-19 crisis.

From the outset of the COVID-19 pandemic, [the EDPS emphasised](#) the need for a pan-European approach in tackling the pandemic. In addition to providing guidance to EUIs, the EDPS closely cooperated with other Members of the European Data Protection Board (EDPB) to offer practical guidance in relation to the most pressing challenges of the pandemic. Among other important points covered in its guidance, the EDPS stressed that pandemic-related technologies requiring the processing of personal data must be temporary, have a defined and limited purpose, and comply with EU data protection law.

Moreover, throughout the first part of 2022, the EDPS has been involved in various activities relating to the assessment of actions, initiatives and proposals by EUIs as controllers, together with the evaluation of proposed technological solutions to fight the COVID-19 pandemic and the issuance of guidance for EUIs in order to assist the EUIs to adequately fight the pandemic, while ensuring compliance with data protection law.

The EDPS was also consulted both informally and formally by the legislator on COVID-19 related legislative initiatives. Amongst such initiatives, the EDPS has issued a Joint Opinion together with the European Data Protection Board (EDPB) on a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/953 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic³, which had the purpose of extending the application of the Regulation (Opinion 1/2022).

2.1.3. Leading by example in safeguarding EU digital rights

In 2022, the EDPS continued its efforts to supervise Union institutions, bodies, offices and agencies' (EUIs) compliance with data protection laws. As outlined in the Strategy 2020-2024, the EDPS is determined to support EUIs to continue to lead by example in safeguarding digital rights and responsible data processing. Examples of several initiatives the EDPS has worked on, and will continue to work on during this mandate, are described below.

1. Strategic actions concerning transfers of personal data outside of EU/EEA after the Schrems II judgment

Following the Court of Justice of the European Union's "[Schrems II](#)" judgment in July 2020 (case C-311/18), the EDPS' launched various initiatives. The EDPS continued to put in place the measures set out in the EDPS' [Strategy for EUIs to comply with the "Schrems II" judgment \(EDPS' Schrems II Strategy\)](#), published on 29 October 2020. The Strategy aims to ensure and monitor compliance of EUIs with the judgment concerning transfers of personal data to non-EU/EEA countries, and in particular, the United States. The strategy builds on cooperation and accountability of controllers as well as on the use of corrective powers, including suspensions and bans of transfers to ensure compliance. As part of the strategy, the EDPS is pursuing three types of actions in parallel: investigations; authorisations and advisory work; and guidance to assist the EUIs in discharging their duty of accountability. Such an extensive exercise in monitoring EUIs compliance with Regulation (EU) 2018/1725 and the reinforced cooperation with EUIs, national Data Protection Authorities (DPAs) and international organisations on transfers, require dedicating special resources and expertise in international transfers.

a) EDPS investigations following the Schrems II judgment

As part of the organisation' enforcement actions following the publication of the [EDPS' Schrems II Strategy](#) in October 2020, the EDPS developed an action plan to streamline compliance and enforcement measures, distinguishing between short-term and medium-term compliance actions.

The Strategy builds on the cooperation and accountability of controllers to assess, in line with the Court's ruling, whether the *essentially equivalent standard of protection* is guaranteed when personal data is transferred to (or remotely accessed by) recipients in non-EU/EEA countries. The EDPS' work in 2022 focused on two priorities that involve

³https://edpb.europa.eu/system/files/2022-03/edpb-edps_1-2022_joint_opinion_on_extension_of_covid_certification_regulation_en.pdf

transfers of data to non-EU/EEA countries: i) EUIs' contracts with private entities, in particular large ICT providers, and ii) arrangements between EUIs and non-EU/EEA public bodies or international organisations.

As part of our Schrems II Strategy, the EDPS focused its investigation activities in particular on EUIs' use of cloud-based services. The use of cloud-based services frequently raises questions related to the role of the providers and data transfers. These are areas where critical compliance issues with Regulation (EU) 2018/1725 and "Schrems II" judgment can occur.

In May 2021, the EDPS had launched two investigations⁴ following the Schrems II judgment. These investigations aimed to ensure that any ongoing and future international transfers by EUIs and on their behalf are carried out in accordance with EU data protection law. One investigation focuses on the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EUIs, while the other investigation focuses on the use of Microsoft Office 365 by the EC. The two investigations were pursued in 2022 and still continue in 2023.

The objective of the first investigation is to assess EUIs' compliance with the "Schrems II" Judgement when using cloud services provided by Amazon Web Services and Microsoft under the so-called "Cloud II contracts" when data is transferred to non-EU countries, in particular to the US. Although the "Cloud II contracts" were signed in early 2020 - before the "Schrems II" judgment - and both Amazon and Microsoft had announced new measures for aligning themselves with the judgment, these announced measures may not be sufficient to ensure full compliance with EU data protection law.

The aim of the second investigation into the use of Microsoft Office 365 was to verify the EC's compliance with the [Recommendations](#) issued by the EDPS in 2020 on the use of Microsoft's products and services by EUIs. This also included compliance regarding international transfers.

In April 2022, the EDPS also issued a [decision](#) about Frontex move to a hybrid cloud consisting of Microsoft Office 365, Amazon Web Services (AWS) and Microsoft Azure, following an investigation initiated in June 2020. The investigation looked at compliance with [Regulation \(EU\) 2018/1725](#), taking into account [EDPS Guidelines on the use of cloud computing services](#) issued in 2018. The EDPS found that Frontex had moved to the cloud without a timely and exhaustive assessment of data protection risks and identification and implementation of appropriate mitigating measures. It also found that the agency had failed to observe the principles of lawfulness and data minimisation. Consequently, a reprimand for a breach of Articles 4(2), 26 and 27 of Regulation (EU) 2018/1725 was issued. The EDPS also ordered the agency to review and amend the data protection impact assessment and the record of processing activities to bring the processing into compliance with Regulation (EU) 2018/1725.

With these investigations, the EDPS aims at helping the EUIs to improve their data protection compliance when negotiating contracts with their service providers. EUIs are well positioned to lead by example when it comes to privacy and data protection. These investigations are part of a continuous cooperation between the EDPS and the EUIs to ensure a high level of protection of these fundamental data rights. The EDPS also aims to

⁴ The EDPS opens two investigations following the "Schrems II" Judgement, 27 May 2021: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en

highlight the need to properly assess the necessity and proportionality of the personal data processing in cloud services, including looking at alternative solutions or providers that entail less interference with fundamental rights.

The EDPS is also cooperating with the data protection *Supervisory Authorities (SAs) of EU and EEA Member States*, by building on the experience set out in the [EDPS' Schrems II Strategy](#). In particular, in 2022, the EDPS actively participated in the [2022 coordinated enforcement action](#) of the EDPB on the use of cloud-based services by public sector bodies. The EDPS focused on the supervision of compliance with Regulation (EU) 2018/1725 when EUIs use such services. The participation in the coordinated action was based on ongoing supervision and enforcement activities of the EDPS, in particular the two ongoing investigations opened following the Schrems II Judgment. In 2022, the EDPS substantively contributed to the work of the working group of DPAs participating in this coordinated action. This was done through the exchange of information gathered during EDPS investigations and other cases, the understanding of the issues found and any examples of best practices with the participating authorities. This allowed for ensuring a common understanding of what public bodies in the EU, including EUIs, must do to comply with EU data protection laws. In particular, the EDPS contributed with regard to the controller-processor relationship and international transfers when public sector bodies use cloud-based services. The findings of the participating DPAs and recommendations for public bodies on use of cloud services were gathered in the [EDPB Report on the 2022 Coordinated Enforcement Action](#)⁵.

b) EDPS authorisations and advisory work

The Schrems II judgment has also complicated the process of issuing authorisations for EUIs that intend to transfer personal data (including by way of remote access) outside of the EEA. The judgment has far-reaching consequences on all legal tools used to transfer personal data from the EEA to any third country and in particular to the United States.

In October 2020, EDPS had strongly advised EUIs against starting any new processing operations or new contracts with any service providers that would involve transfers of personal data to the US.

In 2022 the EDPS reiterated the warning of 2 October 2020 and provided the following guidance to DPOs of EUIs:

- EUIs should not start new processing operations involving transfers, especially to private companies in the U.S.
- In this respect, the new *Transatlantic Data Privacy Framework* announced in April 2022 does not (yet) constitute a legal framework on which data exporters can base their data transfers to the United States.
- EUIs must assess alternatives, e.g. by an EU/EEA organisation, or join the Nextcloud contract re. collaborative tools.

If transfers *cannot be avoided*, the procedural steps should be as follows:

- First, EUIs should consult EDPS informally on any draft administrative arrangements (AA) or standard data protection clauses;
- Only once the EUIs have received the EDPS informal recommendations, they should file the authorisation request (the goal is to avoid multiple back and forth).

⁵ p. 32-40 of the EDPB report contain more information on actions taken by the EDPS.

The EDPS refers the DPOs to the following *tools*:

- As long as there are no adopted EUDPR standard data protection clauses, Art. 46 GDPR Standard Contractual Clauses (SCCs) can be a starting point also for EUIs. The former so called SCCs under Directive 95/46/EC can no longer be used.
- As regards transfers in particular to China, India and Russia, EUIs should take into account the legal study commissioned by the EDPB on government access to data in those third countries⁶.
- In any case, EUIs should be aware that SCCs will likely be not enough and that in many cases, for transfers to private parties, notably in the U.S., it does not seem technically possible to implement effective supplementary measures.

As regards **existing processing operations**, the EDPS indicated that it is the EUIs' responsibility to stop unlawful transfers either by adapting the existing contract or by finding alternative solutions.

In 2022 EDPS provided several **training sessions** on transfers.

It also took a **proactive approach** by supporting the collective effort of EUIs to join the Court of Justice in their negotiations with CISCO regarding the use of Webex for videoconferences, following the EDPS temporary authorisation of September 2021⁷. Moreover, the EDPS is the lead authority in a pilot project regarding the use of collaborative tools involving no transfers outside the EEA (Nextcloud⁸). The package that the EDPS negotiated for "Nextcloud with optional Collabora Office" will be included in the list of group S (SaaS) negotiated packages under the SIDE II Framework Contract.

The EDPS also supports the DPO WG on the Model administrative agreement with International organisations that is being drafted with the involvement of the EU Commission (DG JUST).

EUIs that have to transfer personal data to the US and other third countries need in most cases to request the authorisation of the EDPS. This process, which involves a careful analysis of each case and the inclusion of tailor-made conditions for each authorisation decision as well as their monitoring also require extensive resources and special expertise. In 2022, the EDPS dealt with a number of authorisation requests from EUIs under Article 48 of Regulation (EU) 2018/1725.

(i) Authorisation of administrative arrangements to transfer personal data

1. Decision⁹ on the draft administrative arrangement between SESAR JU and Eurocontrol – (case 2022-0933) – 14 December 2022

The main issue raised by the arrangement relates to oversight and judicial redress mechanisms (a recurring issue with international organisations).

⁶https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en

⁷<https://edps.europa.eu/data-protection/our-work/publications/authorisation-decisions-transfers/edps-decision-authorising-0>

⁸ <https://nextcloud.com/>

⁹ Published: https://edps.europa.eu/system/files/2022-12/22-12-21-decision-temporarily-authorising-the-use-of-the-administrative-arrangement-between-the-single-european-sesar-and-eurocontrol-in-the-context-of-eurocontrols-in-kind_en.pdf

On 14 December 2022, the EDPS issued a decision authorising, until 30 June 2024, the use of an Administrative Arrangement between SESAR (the Single European Sky ATM Research 3 Joint Undertaking) and Eurocontrol (the European Organisation for the Safety of Air Navigation) as a means for adducing appropriate safeguards for transfers between SESAR and Eurocontrol.

Eurocontrol aims to modernise its DP framework by the end of 2023, including on these matters and committed to rely in the meantime on the International Court of Arbitration of the International Chamber of Commerce to provide the function of both oversight mechanism and judicial redress. In light of the transitional nature of this mechanism, the EDPS will have the opportunity to reassess Eurocontrol's future modernised data protection framework, including oversight and redress, hence the temporary authorisation. Should SESAR wish to be allowed to transfer data to Eurocontrol after 30 June 2024, it should file in due time a renewed authorisation, including specific information concerning in particular the modernised data protection framework at Eurocontrol.

2. Decision¹⁰ of 1 August 2022 on the draft working arrangement between Frontex and Niger

EDPS issued a Decision in response to a request for a prior authorisation of a Working Arrangement between the European Border and Coast Guard Agency (Frontex) and the Republic of Niger as a means for adducing appropriate safeguards under Article 48(3)(6) of the Regulation.

The draft Working Arrangement aimed to enable Frontex and Niger to exchange personal data in the context of operational cooperation against irregular migration and cross-border crime. It provided for the exchange of Frontex and national authorities' staff data (for cooperation in capacity building activities, delivery of trainings, and deployment of staff). In addition, the draft Working Arrangement foresaw the exchange of information within the framework of EUROSUR, the European Border Surveillance System (primarily limited to aircraft identification numbers, but with a possibility to extend to other, unspecified, categories of personal data where exceptionally required).

Through its Decision, the EDPS stated that it was not in a position to authorise the use of the Working Arrangement as a means for adducing appropriate safeguards under Article 48(3)(b) of the Regulation.

For considering that the Working Arrangement provides adequate safeguards for the exchange of staff data, the EDPS requested certain changes such as defining modalities for exercising data subject rights, strengthening transparency, safeguards for special categories of data and stricter provisions against onward transfers.

As regards the exchange of data in the framework of EUROSUR, the EDPS found that the draft Working Arrangement did not meet the strict conditions imposed by the Frontex Regulation on transfers of personal data to third countries via EUROSUR. In particular, the Transfer Impact Assessment provided by Frontex indicated risks to the fundamental rights of individuals who may be identified through the transfer of aircraft identification numbers and potential barriers to the exercise of judicial redress for such individuals. The EDPS therefore requested Frontex to remove provisions for the

¹⁰https://edps.europa.eu/system/files/2022-11/2022-0647_updated_redacted_en.pdf

exchange of data within EUROSUR, propose supplementary measures for this transfer, or demonstrate that problematic legislation will not be applied in practice to the transferred data.

The Decision applies EU law on transfers to a particularly sensitive context, namely EU action to extend surveillance of irregular migration and cross border crime in third countries far beyond the EU's external border. It links to the EDPS' wider supervision of Frontex and of EU surveillance targeted at people on the move.

(ii) Authorisation of contractual clauses to transfer personal data

Request for renewal of the Decision authorising temporarily the use of contractual clauses between the Court of Justice of the EU and Cisco for transfers of personal data in the Court's use of Cisco Webex and related services (case 2022-0902) – *Decision adopted on 28/10/2022*

Use of contractual clauses between the Court of Justice of the EU and Cisco Systems Inc. US for transfers of personal data in the Court's use of Cisco Webex and related services. This Decision follows an earlier one issued in August 2021.

Upon verification, the EDPS concluded that although the Court made significant progress towards compliance with the 2021 Decision, there are still areas of non- or partial compliance. The Decision of 28 October 2022 gave the opportunity to reiterate the significance for the operations of the EUIs of Protocol No. 7 to the Treaties on the Privileges and Immunities of European Union¹¹, establishing the inviolability of the archives of the Union. As a result, the EDPS in particular identified the need to for the Court to adapt the GDPR's standard data protection clauses to the specific context of the EUDPR, especially with regard to the disclosure access requests from authorities of third countries.

On 28 October 2022, the EDPS issued a Decision temporarily and conditionally authorising the use of contractual clauses between the Court of Justice of the EU and Cisco.

The Decision authorises until 31 October 2024 the use of contractual clauses. The Court is to remedy the compliance issues identified by the Decision within 16 months i.e. by 1 March 2024. In addition, the Court is to provide the EDPS with an intermediate compliance report 12 months after the date of entry into force of this Decision demonstrating steps taken to implement the conditions set in this Decision, as well as a final compliance report at the expiry of the 16-month deadline to comply.

c) Handling and investigating complaints against EUIs

In 2022, the EDPS created within the Supervision and Enforcement unit a specific "Complaints and Investigation Sector" with staff specifically dedicated to working on complaints and investigations. All of these members of staff have substantial work streams in other areas, such as participating in EDPB subgroups and working on procedural matters.

The EDPS received 65 admissible complaints in 2022. The EUIs concerned were mostly the European Commission, Europol, the EIB and EPSO. The most common issues examined

¹¹ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:310:0261:0266:en:PDF>

were data subjects' right of access and erasure, and proportionate collection of individuals' data.

The EDPS also continued working on unresolved complaints received in previous years. The organisation can handle complaints, and investigate them to the extent necessary, in different ways. A complaint procedure can be concluded either by referral to the DPO of the EU; by referral to a controller in the EU; by amicable settlement or other resolution during the investigation phase; by formal decision or by pursuit of the matter through other EDPS enforcement actions (such as an audit or investigation).

2. Supervision of the Area of Freedom, Security and Justice

As part of its work, the EDPS also supervises the data processing operations of the following bodies and agencies:

- the European Union Agency for Law Enforcement Cooperation (Europol);
- the European Union Agency for Criminal Justice Cooperation (Eurojust);
- the European Public Prosecutors' Office (EPPO);
- the European Border and Coast Guard Agency (Frontex);
- the European Asylum Support Office (EASO);
- the European Union Agency for the Operational Management of Large Scale IT Systems in the Area of Freedom, Security and Justice (euLISA).

These bodies and agencies are part of the Area of Freedom Security and Justice (AFSJ). According to Title V of the Treaty on the Functioning of the European Union, the AFSJ covers policy areas that range from the management of the European Union's external borders to the judicial cooperation in civil and criminal matters. The AFSJ also includes asylum and immigration policies, police cooperation and the fight against crime, such as terrorism, organised crime, trafficking of human beings, drugs.

The legal framework remains fragmented, as the EU has accumulated a patchwork of measures in the areas of police and judicial cooperation and border management, creating unnecessary discrepancies. Still, the EDPS is determined to enforce data protection rules consistently, in line with the general rules contained in the EUDPR, in particular in Chapter IX. Supervision of this area builds on the need to "actively promote justice and the rule of law" as a way to "promote a vision of digitalisation that enables us to value and respect all individuals. The full potential of data shall be dedicated to the good of society and with respect to human rights, dignity and the rule of law.

a) EDPS Order of 3 January 2023 against Europol

The Europol Regulation is framed around the balance between data protection and operational needs. It is framed around a series of key safeguards and the EDPS has been tasked to keep this balance and monitor the implementation of those safeguards.

In this context, the EDPS issued its [Order](#) of 3 January 2022. Concluding the inquiry launched in 2019 regarding Europol's processing of large volumes of individuals' personal data with no established link to criminal activity, the EDPS decided to use its corrective powers and to impose a 6-month retention period for Europol to filter and to extract the personal data. This meant that Europol was no longer permitted to retain data about people who have not been linked to a crime or a criminal activity for long periods with no set deadline. Nevertheless, taking into account the operational needs of Europol and the

amount of data collected so far, the EDPS granted a 12-month period for Europol to comply with the Order for the datasets already received before the latter was notified to Europol.

Throughout 2022, the EDPS closely followed the implementation of the Order and required that Europol submitted quarterly reports evidencing the progress achieved with regard to its implementation and the erasure of datasets that were not compliant with the Europol Regulation. Europol clarified in their second progress report that as of 28 June 2022 (entry into force of the amended Europol Regulation) they process the personal data they hold or receive in line with the amendments to the Europol Regulation, including Articles 74a and 74b, the provisions that retroactively legalised Europol's unlawful practices. The EDPS has however asked Europol to provide a state-of-play on the implementation with the Order, in light of the new applicable provisions, after 28 June 2022.

b) EDPS Court challenge against Art. 74a and 74b amended Europol Regulation

On 16 September 2022, the EDPS for the first time in his institutional history filled an action for annulment and requested that the Court of Justice of the European Union (CJEU) annuls two provisions of the newly amended Europol Regulation, which came into force on 28 June 2022. The two provisions have an impact on personal data operations carried out in the past by Europol. In doing so, the provisions seriously undermine legal certainty for individuals' personal data and threaten the independence of the EDPS - the data protection supervisory authority of EU institutions, bodies, offices and agencies.

These new provisions, articles 74a and 74b, have the effect of legalising retroactively Europol's practice of processing large volumes of individuals' personal data with no established link to criminal activity. This type of personal data processing is something that the EDPS found to be in breach of the Europol Regulation, which it made clear in its [Order](#) issued on 3 January 2022 requesting Europol to delete concerned datasets within a predefined and clear time limit.

The EDPS had to apply for an annulment of these provisions for two reasons. Firstly, to protect legal certainty for individuals in the highly sensitive field of law enforcement where the processing of personal data implies severe risks for data subjects. When data was collected under the previous Europol Regulation, individuals could expect that if their personal data was transmitted to Europol, Europol would be obliged to check within six months whether there was a link to criminal activity. Otherwise, as instructed by the EDPS, this data was supposed to be erased at the very latest by 4 January 2023. Secondly, to make sure that the EU legislator cannot unduly 'move the goalposts' in the area of privacy and data protection, where the independent character of the exercise of a supervisory authority's enforcement powers requires legal certainty of the rules being enforced. The co-legislators' choice to introduce amendments that allow Europol to continue processing the data that has not yet been erased, despite the EDPS Order, undermines the independent exercise of powers by the supervisory authority and establishes a worrying precedent.

c) Europol Management Board Decisions regarding the conditions for processing big datasets lacking Data Subject Categorisation

The amendments to the Europol Regulation that entered into force in June 2022 have shifted the balance between data protection and Europol's operational needs and they considerably expanded the mandate of Europol with regard to the processing of personal data. The extent to which the risks for the data subjects can materialise or be mitigated now lies in the details of the implementation of the new provisions of the amended Europol Regulation. This is why the Europol Management Board Decisions concerning the implementation of Articles 18a and 18(6a) of the amended Regulation are of particular importance. The amended Europol Regulation also required Europol to consult the EDPS prior to the adoption of these Decisions, for ensuring that an independent opinion is provided on the appropriateness of the data protection safeguards defined by Europol.

Aware of the need for Europol to have these rules in place as soon as possible after the entry into force of the amended Europol Regulation, the EDPS provided informal advice on a series of draft texts before the entry into force. However, the decision by the Europol Management Board (MB) to adopt these Decisions on the day of the entry into force of the amended Europol Regulation prompted the EDPS to use for the first time its corrective power of referral of a matter to the Commission, the Council and the European Parliament. The decision to make use of this corrective powers was motivated both because there were important considerations of substance related to the draft MB Decisions which could not be raised during the informal consultation phase, and because the violation by Europol of the essential procedural requirement of consulting the EDPS infringes a provision of institutional nature and deprives the EDPS of his prerogatives to make the decision-making agency reflect and duly consider his opinion before adopting the MB Decisions.

As a consequence, Europol formally submitted to the EDPS the text of the MB decisions for prior consultation on 15 September 2022.

The EDPS in its [Opinion](#) issued on 17 November 2022, identified three areas of concern. The most important concern is the one with regard to the scope of application of new Article 18a of the amended Europol Regulation. According to this provision, Europol can process datasets without an attributed data subject category for the purpose of supporting a specific ongoing criminal investigation upon request of a Member State, EPPO, Eurojust or a third country, and only where the Agency assesses that it is not possible to support the specific criminal investigation without processing those personal data. Europol may process such data for the whole duration of the investigation. After the investigation has been concluded, Europol may store investigative data and the outcome of its processing for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process upon request of the provider of the data and for as long as the judicial proceedings concerning the specific criminal investigation are ongoing.

The EDPS is still waiting for Europol to amend the content of the MB Decisions in line with its Opinion.

d) Monitoring the implementation of the principle of Data protection by design

Data protection by design aims to build data protection and privacy into the design of processing operations and information systems, for comply with data protection

principles. Organisations are required to take into account the protection of the rights of individuals, both before and during their processing activities, by implementing the appropriate technical and organisation measures to ensure that they fulfil their data protection obligations. This requires to have appropriate methodologies and processes in place.

The obligation for controllers to draft Data Protection Impact Assessments (DPIAs) and submit them for prior consultation to the EDPS when the processing involves high risks for individuals (Article 90 EUDPR, Article 72 EPPO Regulation and Article 39 Europol Regulation¹²) participates to the compliance with this obligation and to the fostering of accountability. It remains crucial that, through the DPIA and prior consultation tools, the most risky processing operations in an already sensitive field are properly assessed.

In the context of prior consultations, the EDPS should make an assessment of the compliance of the processing and in particular of the risks for the protection of operational personal data and related safeguards. Supervisory Opinions contain recommendations to avoid non-compliance the applicable data protection framework.

In 2022, the EDPS has focused on the methodology and processes in place to implement data protection *by design* throughout the design of new IT systems and has issued specific recommendations for compliance of data protection obligations at the development stage of several systems and processes in nine Supervisory Opinions following prior consultations.

Methodology and processes applied to the design of new systems

In line with Article 27 and 85 of the Regulation 2018/1725, data protection *by design* (DPbDD) is a requirement for any processing of personal data implemented by an EUI. "Processing" always occurs following a series of processes¹³.

For building a new system, an EUI needs to undergo a phase of software development¹⁴ and testing which are a set of process by which specialised IT staff construct an IT application for meeting the requirements laid out by the end-user of the application¹⁵. Thus DPbDD must be integrated into those processes as well across all systems managed by an EUI and which process personal data.

In the context of software testing and development, this entails that the source code developed and tested will process personal data in such a way as to reduce the risks¹⁶ to the processing of said personal data, by taking into account the EDPB guidelines on DPbDD

¹² The EDPS highlights that the legal framework governing this obligation changed halfway through the year with the adoption of the amended Europol Regulation in June 2022. With this change, the framework for Europol to submit this type of consultation is now identical to the framework that applies to national law enforcement authorities (known mostly as the 'Law Enforcement Directive'), as well as other EUIs who operate in the sphere of Chapter IX of the EUDPR (notably Eurojust and the European Public Prosecutor's Office). The EDPS welcomes this change, as it creates a clear and level playing field for police and criminal justice authorities processing personal data. The EDPS appreciates that the new provision places an increased emphasis on the mitigation of high risks to data subjects by Europol, following the risk-based approach that was introduced by the GDPR and the Law Enforcement Directive previously.

¹³ A set of activities in order to reach a defined goal.

¹⁴ It is possible to acquire a piece of software from a vendor. However, the selection process must also take into account data protection and these usually involve some sort of configuration and testing.

¹⁵ In simpler terms, according to ISO 24765:2017, software development is a "process by which user needs are translated into a software product".

¹⁶ Risks to the data subject whose personal data is processed. This is not to be confused with business/corporate risks of security risks (nor any other types of risks).

i.e. the principles of Transparency, Lawfulness, Fairness, Purpose Limitation, Data Minimisation, Accuracy, Storage limitation, Integrity and Confidentiality, and Accountability are applied to each step of each software development and testing process.

The EDPS has been focussing on ensuring that DPbDD is integrated into these software development and testing processes, not only for new software but also for changes to existing software vis-à-vis Europol, Eurojust and Frontex.

- **NEO - New Environment for Operations (Europol):** On 15 March 2022, the EDPS opened an enquiry on the topic of Europol's NEO given that the EDPS was (and still is) concerned by the piecemeal approach that Europol decided to follow for such a complex and important environment in particular as regard compliance with the fundamental data protection principles envisaged in particular in Articles 28 and 31 of Regulation (EU) 2016/794 ('Europol Regulation') as well as with the principle of DPbDD (Article 33 of Europol Regulation). This is in addition to the yearly Europol inspections performed by the EDPS and which have identified that NEO is the key piece¹⁷ where DPbDD needs to be implemented.
- **New CMS of Eurojust:** Eurojust is currently laying the groundwork to move to a more effective and efficient Case Management System (CMS). The EDPS is looking into the DPbDD aspects of the development of this new CMS. In this case, since a contractor is being used, the approach to implementing DPbDD is different and requires us to examine the data protection elements defined in the business scenarios and market research of the contractor to ensure that DP is taken into account from the get-go.
- **Frontex:** In the context of the Frontex audit, an IT technical team was selected to look into the implementation of the DPbDD principle in particular for the processing of personal data resulting from the activities of screening and debriefing of migrants. From a DPbDD point of view and in Frontex's case, for the development of new IT systems is done via a mixed approach of using contractors and internal development. This required us to both look into the contractors' obligation towards DPbDD and Frontex's way of including DPbDD into their internal development processes.

The EDPS is closely following the changes in Europol, Eurojust and Frontex and working with the staff of these EUI in order to ensure that DPbDD is implemented as thoroughly as possible in all new and existing developments.

Advising on the implementation of data protection obligations

In 2022, the EDPS has issued nine Supervisory Opinions on prior consultation requests submitted by Europol (seven), EPPO (one) and Eurojust (one).

The EDPS issued seven Supervisory Opinions in response to Europol prior consultations on:

- various components of Europol's New Environment for Operations (NEO),
- Europol's process to perform fingerprints- searches in the Schengen Information System (SIS II)¹⁸
- A pilot project for a European Police Records Index System (EPRIS), aiming to establish the capability for the automated searching of police records indexes

¹⁷ This is not to say that DPbDD does not need to be implemented for other systems.

¹⁸ The EDPS released two prior consultation Opinions on this topic.

between its participating Member States, in preparation of the possible adoption of the Prüm II proposal.

- The extension of the existing interface between Member States' systems and the Europol Information System ('EIS'), with (indirect hit/no-hit) access to personal data processed in Europol's Analysis Projects (this new iteration is referred to as QUEST+).
- PERCI, the European Platform for takedown of illegal content online. PERCI, which is the successor of the Internet Referral Management application (IRMa), will provide Member States and Europol with a technical solution for managing referrals and removal orders to hosting service providers for the removal of terrorist content online in line with the provisions of Regulation (EU) 2021/784.

In July 2022, the EPPO submitted a prior consultation on a new environment for operational analysis. This new environment was deemed necessary, as EPPO's case management system (CMS) is not equipped with tools to analyse large case files (i.e. voluminous financial documentation). The Case Analysis Tool Environment (CATE) is a separated and secured environment that allows to import data from the CMS, conduct the analysis and export the results back. Recommendations addressed *inter alia* the issues of data subject categorisation, retention periods and the need to develop policy documents.

Finally, Eurojust submitted two prior consultations, following the adoption of new Eurojust mandate in June, as the agency started to set up a new automated data management and storage facility. This new project called Core International Crimes Evidence Database (CICED) is essential for Eurojust's role as European hub for storing, preserving and analysing evidence of atrocities committed in the Ukraine. Prior consultation of the EDPS is one of important safeguards provided by the legislator, ensuring that such sensitive evidence is processed in line with data protection rules. In agreement with the EDPS, the project is implemented in stages and in 2022 the EDPS was consulted on stage one - transmitting big files from national authorities to Eurojust. EDPS noted with satisfaction that Eurojust's solution for transmission was based on Nextcloud - a privacy friendly platform promoted by the EDPS. Consultation on stage two of the project (storage solution) started in December 2022. The implementation of the CICED project will continue in 2023.

e) Strengthening cooperation with national supervisory authorities in order to develop joint supervision

Joint supervision by the EDPS and national DPAs is key in the AFSJ as EUIs process personal data collected at national level and further shared by competent national authorities for the performance of their tasks. Coordinated supervision ensures that there is no gap in accountability of the different authorities authorised to process personal data about individuals.

The EDPS has been actively participating to the different bodies in charge of ensuring the coordinated supervision of Europol (Europol Cooperation Board until 27 June 2022, Coordinated Supervision Committee from 28 June 2022 on), Eurojust and EPPO (Coordinated Supervision Committee). The [CSC Work Programme](#) 2022-2024 includes several joint supervisory actions to which the EDPS intends to contribute actively. The EDPS continued our joint supervision of the processing of personal data about minors under 15 labelled as "suspects" or "potential criminals" by Europol. This joint supervisory

activity is an ongoing annual activity since 2020, initiated at the initiative of the EDPS on the basis of findings from the 2018 Europol Annual Inspection, which results into national checks for ensuring that the data processed by Europol is in line with the applicable national law, in addition to compliance with the requirements of the Europol Regulation.

In December, the EDPS signed a Working Arrangement with the Portuguese DPA on close cooperation in relation to the exercise of their supervisory and enforcement powers. Both supervisory authorities intend to put this new cooperation framework into use in support of EDPS supervisory tasks in relation to the EPPO.

3. Overview of remote audits

[Audits](#) are an exercise that the EDPS carries out on a regular basis as the DPA of EUIs. Amongst this year's audits, one was carried out remotely due to the COVID-19 pandemic, the rest could again (as in previous years) be carried out on-the-spot (Europol, Frontex and Eurodac, VIS and SIS II information systems at the premises of eu-LISA). The scope of remote audit the EDPS carried out was the processing of personal data in the context of recruitment involving online assessments with remote invigilation (e-recruitment). It focussed on the implementation of existing guidance and covered several EUIs that had notified the existence of such COVID-related processing operations in response to an EDPS Survey.

4. Advising and guiding EUIs

a) Supervisory Opinions and guidance

EUIs may consult the EDPS for guidance on their planned processing operations and on their compliance with data protection law. Depending on the complexity of the EUI's request, the EDPS provides advice in different forms, via calls to the DPO hotline, informal advice to staff and formal signed letters, for example. EUIs may also oblige to consult the EDPS on planned processing operations, particularly when they intend to adopt internal rules restricting individuals' right to data protection and with regard to extra-EU transfers of personal data that require prior authorisation. The EDPS can also issue own-initiative opinions. In total, during 2022 the EDPS issued around 40 opinions.

Covid-19

At the beginning of 2022, the EDPS continued to monitor the COVID-19 situation and its impact on data protection notably through the publication of a report on survey on EUIs' resilience to COVID-19.¹⁹ The report is based on an earlier survey and comprises three parts: new processing operations implemented by EUIs; IT tools implemented or enhanced by EUIs to enable teleworking; and new processing operations implemented by EUIs in charge of tasks related to public health. The dynamic evolution of the COVID-19 pandemic meant that EUIs must continually adapt their processes. The report aims to support them in what appears to be a long-lasting challenge. The survey results are to feed into updating existing EDPS guidelines, or contribute to the development of new guidelines, depending on the evolution of the pandemic and the new practices that will

¹⁹https://edps.europa.eu/system/files/2022-03/22-03-03_covid_survey_rreport_en.pdf
https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-report-eu-institutions-resilience-covid-19_en

continue once it is over. The survey results were also intended to inform the EDPS' execution of audits and investigations under Article 58 of Regulation (EU) 2018/1725.

The EDPS also issued several supervisory opinions in reply to consultations on the digital verification of EU Digital COVID-19 certificates²⁰ for all individuals who access premises of certain EUIs in various Member States. The EDPS issued recommendations in line with previously issued guidelines on the matter²¹.

The EDPS also issued a Supervisory Opinion on the processing of certain health data related to medical vulnerability to COVID-19, both within and outside an EUI's Occupational Health Service²². The *Opinion* highlighted that the EUI [the European Investment Bank (EIB)] should implement suitable and specific measures to safeguard the rights and freedoms of data subjects, ensure that personal data are processed fairly and in a transparent manner and provide data subjects with all relevant information. The *Opinion* also called for a regular review of the retention period, taking into account the dynamic evolution of the epidemiological situation and its scientific understanding.

Apart from COVID-19 related questions, the EDPS issued opinions on a broad range of topics. Here is a selection:

*Clarification of the data protection status of external service providers*²³

The question related to the status of legal advisers and other private service providers vis-à-vis the EIB. In particular, whether they should be considered (joint or separate) controllers or processors. The EDPS clarified that:

- In order for private service providers to only act as processors and for the EIB to maintain controller over processing, the EIB should provide sufficiently detailed instructions as to the processing of personal data wherever this is feasible.
- When acting as a controller, the EIB should ensure that the contract or another legal act under Article 29(3) EUDPR takes into account the specific tasks and responsibilities of the processor and the risk to the rights and freedoms of data subjects.
- Since some service providers are based outside of the EU, the EIB should ensure compliance with Chapter V EUDPR as regards transfers of personal data to third countries.

*Restricting individuals' rights*²⁴ - European Central Bank (ECB) (5/10):

This Supervisory Opinion relates to internal rules of the ECB restricting data subjects' rights, in accordance with Article 25(4) of the EUDPR, which regulates data processing for archiving purposes in the public interest. The EDPS stated that the ECB should:

- ensure that it provides information to individuals about the subsequent transfer of their personal data to the historical archives at the same time of providing information about the processing of their personal data when it is initially collected;

²⁰ https://edps.europa.eu/system/files/2022-01/22-01-07_edps_opinion_ec_draft_decision_covid_certificates_lux_en.pdf (EC in Luxembourg); https://edps.europa.eu/system/files/2022-03/22-02-11_edps_opinion_covid_vaccination_pass_ispra_en.pdf (EC JRC in Ispra, Italy); - https://edps.europa.eu/system/files/2022-05/2022_03_01_formal_consultation_covid_certificate_en.pdf (EP Strasbourg, Brussels and Luxembourg)

²¹ https://edps.europa.eu/system/files/2021-08/21-08-09_guidance_return_workplace_en_0.pdf

²² https://edps.europa.eu/system/files/2022-03/22-02-17_formal_opinion_health_covid19_en_0.pdf (EIB)

²³ https://edps.europa.eu/system/files/2022-04/22_04_06_opinion_private_service_providers_en.pdf

²⁴ https://edps.europa.eu/system/files/2022-10/22-10-05_edps_supervisory_opinion-historical-archives_en.pdf

- introduce an obligation to consult the DPO before the controller takes any decision to derogate from data subject rights in a particular case;
- involve the DPO throughout the procedure and document this consultation;
- introduce an obligation to record any derogations applied pursuant to the draft Decision, as well as the reasoning that justifies the derogation. In other words, the controller should document why it is necessary to derogate from data subject rights in a particular case.

Processing of personal data in competition law investigations

In May 2022, the EDPS issued a supervisory opinion on processing of personal data in the context of competition law investigations.

In the Supervisory Opinion, the EDPS highlighted that the relevant provisions of Regulation (EU) 2018/1725 and competition law (i.e. Regulations (EC) No 1/2003 and No 773/2004) should be applied in a manner that is mutually compatible and enables them to be applied consistently.

Employee data - Activity recording tool²⁵

The consultation related to the deployment of an activity-recording tool to fulfil Eurojust's reporting obligations related to the utilisation of human resources per activity and refine the planning of human resources. The EDPS Supervisory Opinion recommends that Eurojust:

- adopt an executive decision stating the exact terms of this processing operation;
- double-check if the specificity of the activities and the size of the Units allow for the singling out of individuals and adapt the information provided to the staff (data subjects) accordingly;
- update the legal framework in the contract entered between Eurojust and the processor, as well as with the sub-processor.

b) Training EUI staff on protecting personal data in their tasks

The EDPS routinely carries out a number of training sessions every year. During 2022, the EDPS gave a series of online advanced lectures at the European School of Administration (EUSA) and other venues for staff members of all EUIs and their DPOs concerning transfers of personal data by EUIs or on their behalf. Almost all training sessions were carried out remotely.

An online training session was held on transfers of personal data to non-EU/EEA public bodies and organisations and two sessions on the conditions and data protection safeguards for transfers to non-EU/EEA private entities. Transferring personal data to non-EU/EEA countries may present additional risks for individuals, as these countries may not have the same legislation put in place to ensure that personal data is adequately and sufficiently protected. This is why when transferring individuals' personal data to countries outside the EU/EEA, EUIs have to ensure that the level of protection offered by the country of destination offers an essentially equivalent level of protection as in the EU/EEA. During the training sessions, the EDPS experts gave recommendations on how EUIs need to carry out Transfer Impact Assessments and put in place effective

²⁵ https://edps.europa.eu/system/files/2022-10/22-04-04-edps-opinion-2021-0808_en_0.pdf

supplementary measures to ensure an essentially equivalent level of data protection as in the EU/EEA for the data that will be transferred to that recipient in that third country. The EDPS experts emphasised that if no essentially equivalent level of protection is guaranteed by a country of destination, then the transfer of individuals' personal data to that country should not occur.

The EDPS regularly organises training sessions and lectures on challenging topics, such as the topic of international data transfers, for EUIs, their DPOs, and their members of staff. These training sessions, either organised by the EDPS' own initiative, or at the DPO's request, aim to ensure that EUIs stay up to date with data protection regulation and requirements in their day-to-day activities.

Throughout 2022, the EDPS gave 22 trainings and presentations to EU staff and to external persons (i.e students, judges etc)

Delivering training sessions to European institutions, bodies, offices and agencies (EUIs) and providing them with the necessary tools to protect individuals' personal data in data processing activities are an integral part of how the EDPS monitors EUIs' compliance with data protection laws.

In 2022, the EDPS launched a Learning and Development Plan (L&D Plan) for members of staff of EUIs. The L&D Plan includes a series of online training courses and recorded online talks on data protection and on how to apply Regulation (EU) 2018/1725. These recorded online talks, were prepared in collaboration with the EUSA: https://edps.europa.eu/press-publications/publications/newsletters/newsletter-93_en#learning.

Training sessions are usually recorded and made available to all staff of EUIs in the inter-institutional learning platform EU Learn. The new recordings will be added to the L&D Plan prepared by the EDPS and EUSA. These training sessions deal with areas in which further clarity or assistance to ensure compliance with Regulation 2018/1725 is required. For example, the EDPS organised several training sessions on EUIs' use of social media, on data protection in procurement and outsourcing, on data subject rights, and on data protection impact assessments. In addition, the EDPS also organised on-demand training sessions requested by EUIs and their DPOs, focusing on data protection operations and their implications in relation to the EUI's core activities and area of business. The training sessions by the EDPS include expert presentations on the subject, case studies and practical examples that staff of EUIs may encounter in their daily work.

Other factsheets on this topic, as well as many other pertinent subjects relevant for EUIs, were published on the EPDS website in 2022, such as : "[Your data, your rights](#)" on data subjects' rights . This practice will continue in 2023 as it is an efficient and accessible way to support DPOs of the EUIs.

In 2022, the EDPS continued to publish our "Quick News for DPOs" editions, a monthly newsletter for data protection officers of the EUIs. The DPO newsletter was created in 2019 for staying in touch regularly with DPOs to foster good communication and collaboration. The newsletter provides DPOs with the latest updates on EDPS Guidelines, Recommendations or Opinions directly relevant to their day-to-day work, their EUI's core business and current data protection developments that concerns them or their institution. While preserving the anonymity of the EUI in question, the EDPS also shares information about common questions, complaints or consultations that may have been received from an EUI, as these can help DPOs to know what measures to put in place if

they encounter a similar situation. Ten editions of the DPOs Quick News were published in 2022. Some of the topics covered throughout the year include: basic data protection principles; transfers of personal data to non-EU/EEA countries; protecting individuals' data in the context of recruitment; how to handle employees' data in the context of a pandemic. The newsletter is also used to promote upcoming training sessions or events organised by the EDPS for DPOs and other members of staff of EUIs, which DPOs are always encouraged to join. Each edition also includes a data protection recommendation of the month.

The EDPS has also developed a Wiki including an annotated Regulation 2018/1725 available to DPOs. The Wiki, which includes links to EDPS published Opinions and decisions, EDPB/EDPS Guidelines, CJEU case law, provides a precious source of information for DPOs in their daily tasks.

5. EDPS meetings with the network of DPOs

Due to the important role played by DPOs as interlocutors between the EDPS and EUIs, a biannual meeting is held to discuss current and upcoming data protection challenges. This provides an opportunity to realign data protection priorities for the DPOs of EUIs and to identify areas where extra guidance or support from the EDPS is needed. In 2022, a group of DPOs, the DPO Support Group, actively contributed to the organisation of both EDPS - DPO Meetings in 2022, by suggesting topics for the agenda, preparing case studies and co-facilitating workshops at the EDPS-DPO meeting. The DPO Support Group's commitment and hard work contributed to making both meetings a success.

DPO meetings (50th and 51st):

- on 14 June 2022 in Brussels https://edps.europa.eu/press-publications/publications/newsletters/newsletter-95_en#dpo

- on 6 December 2022 in Lisbon https://edps.europa.eu/press-publications/press-news/blog/reiterating-our-commitment-support-data-protection-officers-eu-institutions_en

2.1.4. Shaping a safer digital future for the EU

Throughout 2022, the EDPS closely examined technological developments and multiple initiatives with a meaningful technology footprint and impact on data protection presented by the EU's legislators as well as the use of technology by the EUIs. The EDPS places importance on analysing the possibilities, risks and challenges that upcoming technologies and other initiatives may have on data protection and individuals' personal data for shaping a safer digital future for the EU, as explained in the EDPS Strategy 2020-2024. An overview of several examples demonstrating this are provided below.

Monitoring technologies

- ***Artificial intelligence and Facial Recognition***

Artificial Intelligence (AI) is a reality and has woven its way into everyday life: virtual voice assistants, facial recognition, spam filters and recommender systems to name but a few.

Of the whole set of technologies the term AI encompasses, machine-learning is possibly the subset with most significant advancements. Machine-learning techniques generally rely on big datasets to achieve good performances. If machine-learning system results are to be applied in a European context, it is also necessary to train them with datasets that are representative of such context. This is creating and increasing thrust to collect and process data (personal and non-personal) for the AI system development. The increased processing of personal data in turn present challenges for privacy and data protection.

The EDPS is a member of the Global Privacy Assembly (GPA), the organization that gathers DPAs around the globe. In 2022, the EDPS, jointly with the French DPA, continued to chair the GPA working group on Ethics and Data Protection in AI (AIWG). The EDPS was co-drafter and sponsor of the [Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology](#), adopted in the GPA of 2022.

In 2022, the Council of Europe (CoE) created the Committee on AI (CAI) and tasked it to elaborate a Convention on the development, design, and application of AI systems based on the CoE's standards on human rights, democracy and the rule of law, and conducive to innovation. The EDPS is part of the EU Delegation and as such participated in the discussions that took place in the first and second plenaries of the CAI.

- ***Contribution to the debate on Digital Sovereignty: leading by example***

Following the effort started in 2021, with the organisation of a panel at the Computers, Privacy and Data Protection (CPDP) entitled "Enhancing Personal Data Protection through Digital Sovereignty", the EDPS continued its contribution in this area.

The EDPS launched in April 2022 the public pilot phase of two social media platforms: EU Voice and EU Video.

EUIs participating in the pilot phase of these platforms are able to interact with the public by sharing short texts, images and videos on EU Voice and by sharing, uploading, commenting videos and podcasts on EU Video.

The two platforms are part of decentralised, free and open-source social media networks that connect users in a privacy-oriented environment, based on Mastodon and PeerTube software. By launching the pilot phase of EU Voice and EU Video, the EDPS aims to contribute to the EU's strategy for data and digital sovereignty to foster Europe's independence in the digital world.

Beyond that, the EDPS has been preparing a pilot to use the collaborative platform Nextcloud for drafting documents with multiple authors at the same time. Nextcloud also provides a video conferencing system based on free software. This pilot is expected to be launched in 2023.

- ***Memorandum of Understanding with ENISA***

The EDPS and the European Union Agency for Cybersecurity (ENISA) signed in December 2022 a Memorandum of Understanding (MoU) which establishes a strategic cooperation framework between them.

Both organisations will collaborate designing, developing and delivering capacity building, awareness-raising activities, as well as cooperating on policy related matters on topics of common interest, and contributing to similar activities organised by other EUIs (Cybersecurity of EUIs: EUIBAs).

The MoU includes a strategic plan to promote the awareness of cyber hygiene, privacy and data protection amongst EUIBAs. The plan also aims to promote a joint approach to cybersecurity aspects of data protection, to data protection compliance in cybersecurity operations, to adopt privacy-enhancing technologies, and to strengthen the capacities and skills of EUIBAs.

Internet Privacy Engineering Network (IPEN)

The EDPS founded the [Internet Privacy Engineering Network \(IPEN\)](#) in 2014 to bring together experts from a range of different areas and to encourage the development of engineering solutions to privacy problems. Through facilitating exchange between regulators, researchers and developers who build privacy into new and existing digital tools, IPEN aims to promote and advance state-of-the-art practices in privacy engineering. In 2022, the EDPS held two IPEN workshops, a hybrid one on the technological choices to design digital identity frameworks and their impact on individuals' privacy, and an online one on central bank digital currency to understand relevant challenges and identify the state of the art of the available design options.

IPEN workshop on Digital Identity, Warsaw, June 2022

The EDPS and the Cardinal Stefan Wyszyński University organised on 22 June 2022 an IPEN workshop on Digital Identity in Cardinal Stefan Wyszyński University, Warsaw.

The workshop contributed to the debate on organisational and technological choices to design digital identity schemes and portfolios of personal attributes for digital authorisation purposes that can fully implement the GDPR principle of DPbDD.

The workshop aimed at understanding the challenges and identifying the state of the art of the available options for compliant and privacy-enhancing solutions.

IPEN webinar on central bank digital currency, December 2022

The EDPS organised on 1st December 2022 an IPEN webinar entitled: IPEN webinar on central bank digital currency.

The workshop contributed to the debate that countries around the world are having about whether they should offer central bank money to the public not only as banknotes and coins but also in digital form. While almost 90% of central banks around the world have already launched a state-owned digital currency with different design choices the ECB decided to start an exploratory phase by 2024. Data protection and security are among the most compelling aspects that impact the core design choices to be taken.

The workshop aimed at understanding the challenges and identifying the state of the art of the available design options in the field of transaction validation, auditability and monitoring for compliant and privacy-enhancing solutions.

TechDispatches

The EDPS continued to publish [TechDispatches](#) to explain emerging developments in technology. Each TechDispatch provides factual descriptions of a new technology, preliminarily assesses the possible impact upon privacy and the protection of personal

data, as understood now, and provides links to further recommended reading. In 2022, the EDPS published one TechDispatch focusing on Federated Social Media Platforms that gave an overview of their main characteristics and privacy benefits.

TechSonar

In 2022 the EDPS continued its TechSonar initiative, with the aim to examine which technologies are worth monitoring to be prepared for a more sustainable digital future where the protection of personal data is effectively guaranteed. While the EDPS TechDispatch reports continue to provide in-depth analysis on emerging technologies, they aim to anticipate technology trends.

TechSonar falls within the Foresight pillar of the EDPS Strategy and is a process that empowers the organisation to continuously analyse the technology arena with the aim of selecting tech trends we foresee for the following year. The first publication of the TechSonar reports focuses on topics such as synthetic data, smart vaccination certificates, *just walk out* technology and biometric continuous authentication.

In the context of the wider strategy on technology monitoring, the EDPS has decided to use foresight tools for the main purpose of “closely examining both the potential risks and opportunities offered by technological advances, understand the possibilities of new technologies and, at the same time, encourage the integration of data protection by design and data protection by default in the innovation process”. TechSonar²⁶ is the first project of the EDPS in this field, aiming to identify emerging technologies in the short time window of one year. The decision to select such a small time frame is guided by the need to have an immediate return in the technological preparedness of the officers involved in activities occurring on a daily basis.

Based on the fundamental pillar that guides its work – namely, independence – the EDPS developed an inclusive and agile foresight methodology process that leverages on collective intelligence and increases the collaboration between internal departments.

The first TechSonar Report 2021-2022²⁷ was published in December 2021, with its own dedicated section in the EDPS website²⁸. The second deployment of the project took place in November 2022.

Techsonar Report July 2022 (Enrichment with TIM Analytics)

This new release of TechSonar was enriched with a proof-of-concept analysis tool, created together with the publicly accessible Competence Center on Text Mining and Analysis of the European Commission's Joint Research Centre. The tool supports the information collection process, analysing the most important academic papers, as well as patents and projects funded by the European Union that concern the technologies we selected.

TechSonar is just a first step towards a wider, forward-looking perspective on our future. We are convinced that an effective approach to data protection regulation needs to take into account anticipatory and proactive ways to tackle the supervisory and advisory tasks and to support the value-creation process of privacy enhancing technologies. The use of anticipatory and foresight techniques should be the “new normal” in our future data protection efforts.

²⁶ https://edps.europa.eu/press-publications/publications/techsonar_en

²⁷ https://edps.europa.eu/system/files/2021-12/techsonar_2021-2022_report_en.pdf

²⁸ https://edps.europa.eu/press-publications/publications/techsonar_en

TechSonar Report November 2022 (2022-2023 report)

The November edition summarised the efforts carried out during the year. The EDPS shared its work and discussed it through the co-organisation of the closing conference of the Panelfit project on 31 March 2022, the participation in a panel dedicated to anticipatory techniques at the Computer Privacy and Data Protection conference on 24 May 2022, and the discussion of the EDPS preliminary achievements at the 30th European Conference of DPAs in Dubrovnik on 20 May 2022.

Foresight was also one of the main themes of the EDPS conference on “The Future of Data Protection: Effective Enforcement in the Digital World” which EDPS organised on 16 & 17 June 2022, in Brussels and online.

Continuing on this path, in November 2022 the EDPS issued the second edition of the TechSonar report with an updated set of technologies that was considered to be of primary importance to increase the preparedness of stakeholders in the field of personal data protection: metaverse, fake news detection Central Bank Digital Currency (CBDC), , synthetic data, federated learning.

Personal Data Breaches

EDPS in 2022 continued to monitor and supervise the EUIs on the handling procedures (keeping of registry, assessment of the risk, notification to the EDPS, notification to the data subjects etc) of personal data breaches²⁹ and ensured the protection of fundamental rights and freedoms of the data subjects that were impacted by security incidents that led to a personal data breach.

In 2022 the EDPS initiated the update of its Data Breach Notification Guidelines issued in 2018, with a goal to provide more guidance on how to assess the level of risk of a personal data breach, as well as provide more examples. In this context, two workshops with the DPOs network were held (one online and one during the DPOs meeting in Lisbon in December 2022). The workshops focused on upcoming updates on the EDPS Guidelines and on how to notify personal data breaches to the EDPS and gave rise to fruitful discussions and helpful feedback from the DPOs. The Technology and Privacy Unit (T&P Unit) will continue this work in 2023.

In the context of providing practical information to EUIs on assessing and notifying personal data breaches, the EDPS organised in 2022 two online talks in cooperation with the European School of Administration (EUSA). These sessions aimed at raising employees of EUIs’ awareness on how to prevent or manage personal data breaches and covered the most frequent scenarios in which a personal data breach may occur, such as addressing a letter or an email to the wrong recipient, as well as more complex context, errors when handling transparency and access to document procedures. A similar, tailored training was organised in the EP, for the Directorate-General for Communication. Training sessions provide EUIs’ employees and data protection officers, ideas on how to minimise or avert risks in some of these situations.

In 2022, the EDPS received and assessed 95 new personal data breach notifications under Regulation (EU) 2018/1725. Overall, there was a slight increase (around 9%) in the numbers of personal data breach notifications the EUIs notified the EDPS compared to the figures of 2021. The EDPS also received, in addition to that number, 14 personal data

²⁹ Under Regulation (EU) 1725/2018 all EUIs have a duty to report personal data breaches to the EDPS, unless a risk to the affected individuals is unlikely. These obligations apply also for breaches on operational personal data

breach notifications that were assessed as not personal data breaches. Out of 95 notifications, 52 were comprehensive and 43 were notifications in phases (further notifications were submitted in 2022 and some of them are still pending as investigations are on-going).

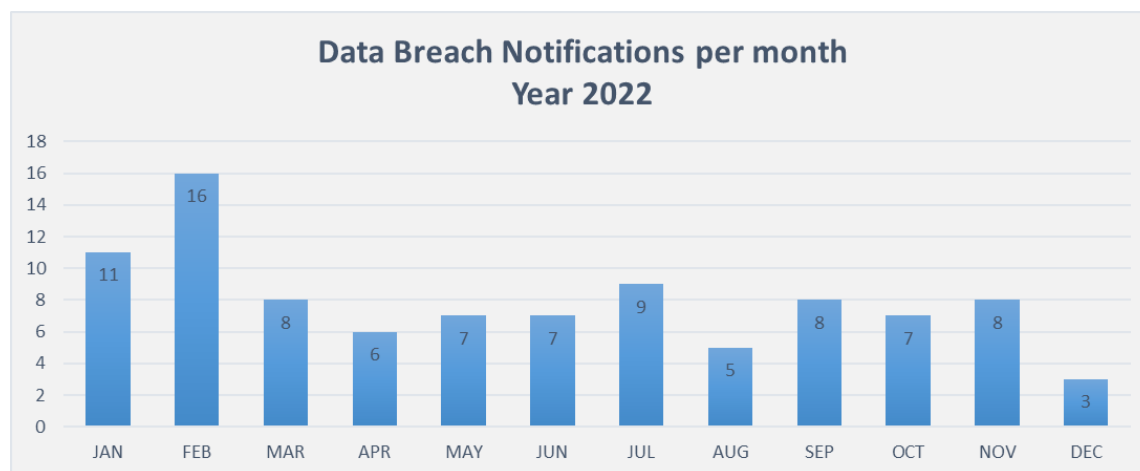


Figure 1 - Graph x Data Breach Notification in numbers 2022

Large Scale IT Audits

Following the relevant legal instruments the EDPS shall ensure that an audit of the Management Authority's (eu-LISA) personal data processing activities is carried out in accordance with international auditing standards at least every four years for the Schengen Information System (SIS II) and Visa Information System (VIS) and every three years for the Eurodac system. Complying with this obligation, 2022 was the year when all those three systems required an audit from the EDPS, which we carried out in October 2022 at eu-LISA. The results are planned by Q1 2023.

Legislative Consultation

The EDPS provides guidance on proposed legislation to the EC, as the institution with the right of legislative initiative, and the EP and the Council, as co-legislators. Our guidance may take the form of:

- **Opinions:** Opinions are issued in response to mandatory requests by the EC, which is legally obliged to seek EDPS guidance on any legislative proposal, or draft implementing or delegated acts, as well as recommendations and proposals to the Council in the context of international agreements according to Article 42(1) of Regulation (EU) 2018/1725³⁰.
- **Formal Comments:** similar to the Opinions, the Formal Comments are issued in response to a request from the EC under Article 42(1) and address the data protection implications of legislative proposals. However, they are usually shorter and more technical, or only address certain aspects of a proposal. Formal Comments are published on the EDPS website.
- **Informal Comments:** the EC is encouraged to consult the EDPS informally before adopting a proposal, which has an impact on data protection. This allows the EDPS to provide the EC with input at an early stage of the legislative process,

³⁰ Opinions, as well as their summaries in all official languages of the EU, are available on the EDPS website and published in the [Official Journal](#) of the EU. Opinions highlight our main data protection concerns and recommendations on legislative proposals or other measures. They are issued in response to a request from the Commission and are addressed to the EU co-legislator.

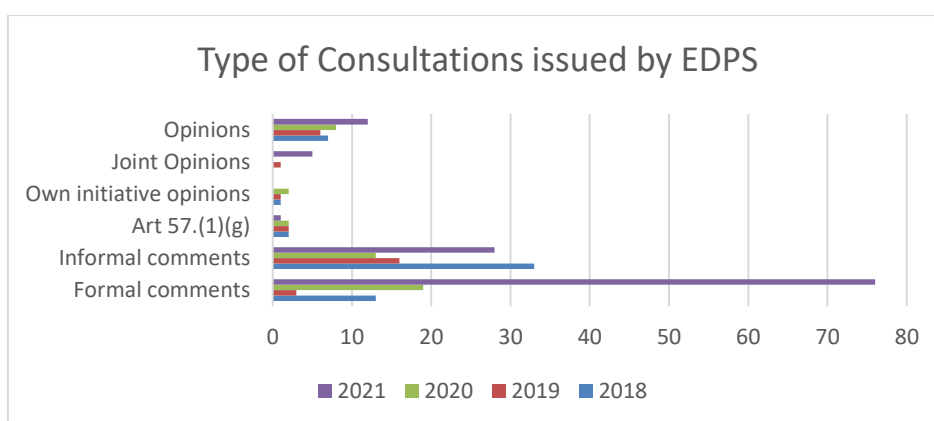
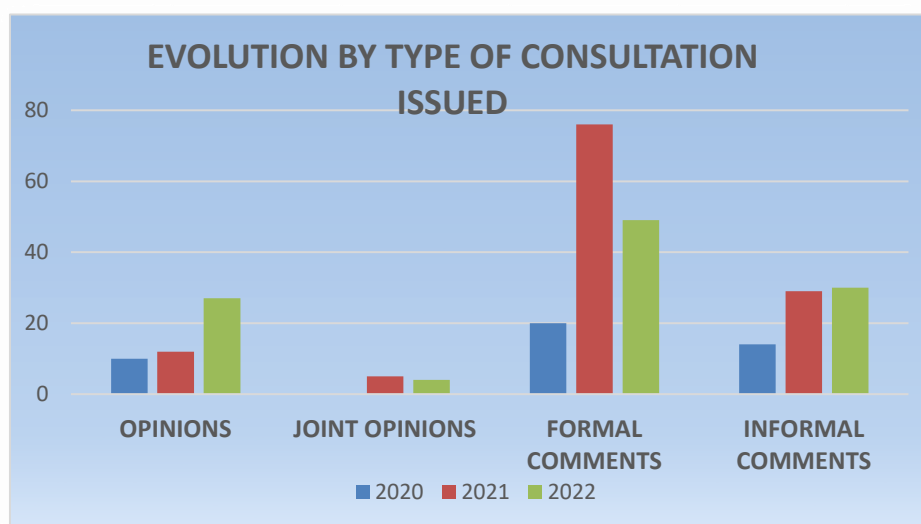
usually at the stage of the inter-service consultation. Informal Comments are, in principle, not published.

- **Joint EDPS-EDPB Opinions:** where a legislative or other relevant proposal is of particular importance for the protection of personal data, the EC may also consult the EDPB. In such cases, the EDPS and EDPB work together to issue a joint opinion³¹.

A significant number of legislative consultations

The statistics provided below clearly demonstrate that the number of requests for legislative consultation has remained significantly high in 2022. There was also an increase in the number of opinions published in 2022³².

The evolution in legislative consultation activities is shown on the following graph:



³¹ See also Article 20 of the EDPS Rules of Procedure.

³² Since the beginning of 2022, the EDPS no longer issues Formal Comments in response to requests for legislative consultation that concern a proposal for a legislative act or a recommendation or proposal to the Council pursuant to Article 218 TFEU, which explains the relative increase in the total number of Opinions and relative decrease in Formal Comments in 2022. This practice has been reflected in the updated EDPS Rules of procedure. See Decision of the European Data Protection Supervisor of 14 October 2022 amending the Rules of Procedure of the EPDS of 15 May 2020, O.J. 24.10.2022 L 274/80.

	2020	2021	2022
OPINIONS	10	12	27
JOINT OPINIONS	0	5	4
FORMAL COMMENTS	20	76	49
INFORMAL COMMENTS	14	29	30
TOTAL	44	122	110

In 2022, the EDPS responded to **76 formal legislative consultations** pursuant to Article 42(1), issuing 27 opinions and 49 formal comments. In addition, **4 joint opinions** were adopted with the EDPB pursuant to Article 42(2) EUDPR. Additional cooperation and coordination is required for joint opinions with the EDPB.

The statistics for 2022 also reflect an increased expectation on the Commission's services side that the EDPS should be involved and **provide advice at the informal stage of preparation** of legislative/policy proposals (i.e. even before the informal consultation stage)³³. This includes: attending workshops, expert meetings and sometimes inter-service meetings, responding to public consultations or targeted consultations or providing inputs to external studies. In this context, the EDPS issued **30 informal comments** in 2022, in addition to other forms of providing informal assistance.

Timelines vary from a few days in the case of an urgent consultation to eight weeks for an opinion on a legislative proposal or an opinion on a prior consultation (according to Regulation (EU) 2018/1725). These short timelines, and the large number of cases in relation to the small size of the EDPS, necessitate careful planning and monitoring to allow planning and executing other, proactive activities, so far as possible within these constraints.

The high number of the legislative consultation activities has kept the translation costs for Policy and Consultation Unit high.

Increased number of follow-up requests

Growing awareness of data protection issues also results in requests from EP, its committees (LIBE, IMCO) and/or individual (shadow) rapporteurs for comments or opinions on compromise amendments or possible outcomes of trilogue negotiations. A new and increasing phenomenon are invitations from relevant working parties of the Council to present EDPS opinions. The Supervisor and EDPS staff regularly respond to such invitations and requests.

While the Unit within the EDPS in charge of legislative consultation has grown slightly since 2018, its increase in staffing is still not commensurate to the overall increase of workload. The substantial increase in consultation requests is also one of the main reasons why there has been a decrease in the number of own-initiative opinions issued by the EDPS.

2.1.5. The EDPS as a member of the EDPB

The [European Data Protection Board](#) (EDPB) is an independent body established under the GDPR that promotes cooperation between national DPAs to ensure the consistent application of data protection rules across the EU. The EDPS is both a member of the EDPB and the provider of an independent Secretariat, which offers administrative and logistic

³³ See recital 60 EUDPR.

support, performs analytical work and contributes to the EDPB's tasks. A [Memorandum of Understanding](#) determines the terms of cooperation between the EDPS and the EDPB.

Much of the work carried out by the EDPB takes place within expert subgroups, each of which covering a specific range of topics. These include key provisions of the GDPR, international transfers, technology and financial matters, among many others.

The EDPS is formally coordinating the Key Provisions Expert Subgroup. In this context, the EDPS consistently plays a leading role as a lead rapporteur, co-rapporteur, or a member of the drafting team.

As a member of the EDPB, the EDPS contributed to multiple EDPB initiatives in 2022, including:

- [EDPB-EDPS Joint Opinion 1/2022 on the extension of the Covid-19 certificate Regulation](#);
- [EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data \(Data Act\)](#);
- [EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space](#);
- [EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse](#);
- [EDPB response to French associations on the cookie consent requirement](#);
- [EDPB response to Mr Juan Fernando López Aguilar regarding the request for an EDPB opinion on the final draft of the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence](#);
- [Toolbox on essential data protection safeguards for enforcement cooperation between EEA data protection authorities and competent data protection authorities of third countries](#);
- [EDPB Rules of Procedure amendment on notification and translation of binding decisions according to Art. 65 GDPR](#);
- [Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement](#);
- [EDPB letters to the European institutions on the protection of personal data in the AML-CFT legislative proposals](#);
- [Guidelines 07/2022 on certification as a tool for transfers](#);
- [Response of the EDPB to the European Commission's targeted consultation on a digital euro](#);
- [Statement 02/2022 on personal data transfers to the Russian Federation](#);
- [Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited \(Instagram\) under Article 65\(1\)\(a\) GDPR](#);
- [EDPB Letter to MEP In't Veld on the use of statistics on Passenger Name Record \(PNR\) data](#);
- [Statement 03/2022 on the European Police Cooperation Code](#);
- [Open letter on EDPB budget proposal for 2023](#);
- [Coordinated Enforcement Framework 2023 – selection of topic](#);
- [EDPB Letter to the EU Commission on procedural aspects that could be harmonised at EU level](#);
- [Statement 04/2022 on the design choices for a digital euro from the privacy and data protection perspective](#);
- [Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority](#);
- [Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service \(Art. 65 GDPR\)](#);
- [Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish](#)

[Supervisory Authority regarding Meta Platforms Ireland Limited \(Instagram\) under Article 65\(1\)\(a\) GDPR;](#)

- [Decision 05/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority re WhatsApp \(WhatsApp Ireland Limited\) according to Art. 65\(1\)\(a\) GDPR](#)
- [Statement on the implications of the CJEU judgment C-817/19 on the use of PNR in Member States.](#)

2.1.6. International cooperation in data protection

As data flows across borders, there is a need to consider data protection in a global context.

In 2022, the EDPS actively participated in a number of international fora with the aim of sharing information and good practices, finding common ground and developing guidance, and working together to improve the understanding of data protection law.

Examples of fora or international conferences that the EDPS has participated in throughout 2022 are presented below.

Global Privacy Assembly

The EDPS is an active member of the [Global Privacy Assembly](#) (GPA) (previously known as the International Conference of Data Protection and Privacy Commissioners, ICDPPC) and former host of the 2018 Conference that gathered more than 1000 delegates discussing digital ethics and the challenges of a data driven society.

The 44th GPA took place between the 25th and 28th of October 2022. The conference was hosted by the Personal DPA of Turkey (KVKK), in Istanbul, and brought together more than 90 members and observers to consider key data protection challenges. The conference started with an Open Session (25 and 26 October) and ended with the Closed Session (27 and 28 October).

During the Closed Session, a series of [Resolutions](#) were discussed and agreed at the conference on a very important topics such as:

- [Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology;](#)
- [Resolution on International Cooperation Capacity Building for Improving Cybersecurity Regulation and Understanding Cyber Incident Harms ;](#)
- [Resolution to Amend the Road Map and the Timeline](#) towards a funded permanent GPA Secretariat.

In addition, in 2022, the EDPS followed the activities and provided substantive contributions to the following GPA's working groups:

- Global Frameworks and Standards Working Group.
- Digital Economy Working Group.
- Data Protection and other Rights and Freedoms Working Group.
- Digital Education.
- International Enforcement Cooperation
- Digital Citizen and Consumer.
- Data Sharing Working Group.

- Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management.
- Data Protection Metrics.

Council of Europe (CoE)

The EDPS also follows the activities of the Consultative Committee of the Convention 108 (T-PD) and represents the GPA before the T-PD. The EDPS participates in T-PD as an observer. The EDPS role involves ensuring a high standard of data protection and compatibility with EU data protection standards.

The activities of the T-PD are diverse and concern topics of strategic impact for the EDPS (facial recognition, artificial intelligence, digital contact tracing, oversight by intelligence services, digital identity, processing of personal data in the context of political activities and elections, contractual clauses in the context of trans-border data flows, inter-state exchanges of data for Anti-Money Laundering/Countering Financing of Terrorism, and tax purposes, etc). With the modernisation of the Convention 108, a very important and strategic follow-up mechanism to the Convention will be created which will also create additional tasks for the T-PD.

Still at the CoE, the EDPS is participant to meetings of the Committee on Artificial Intelligence (CAI) that has been tasked by the Committee of Ministers of the CoE to elaborate a Convention on the development, design, and application of artificial intelligence systems based on the CoE's standards on human rights, democracy and the rule of law, and conducive to innovation.

Organisation for Economic Co-operation and Development (OECD)

The EDPS is also following the activities of the OECD in particular the activities of the Working Party on Data Governance and Privacy (DGP) and Privacy Guidelines Expert Group (PGEG). The work of the OECD is becoming increasingly relevant for the EU and the EDPS. For instance, the OECD ministerial meeting that was held on 14-15 December 2022 led to the adoption of two Declarations: a Declaration on a Trusted, Sustainable and Inclusive Digital Future and a Declaration on Government Access to Personal Data Held by Private Sector Entities. Some of these activities are of strategic importance for the EDPS.

Cooperation with International organisations

Generating and fostering global partnerships in the field of data protection is a priority for the EDPS. One of the ways in which we do this is by co-organising a yearly workshop dedicated to data protection within international organisations. The workshop is a forum for the exchange of experiences and views on the most pressing issues in data protection faced by international organisations all over the world. The size and the relevance of this event has been growing since the first edition in 2005. This confirms the need for a platform for international organisations to engage, share best practices and discuss unsolved dilemmas, and demonstrates the increasing awareness of the importance of ensuring strong safeguards for personal data.

On 12-13 May, the EDPS co-organised with the World Food Programme the 2022 edition of the International Organisations workshop, in Rome, Italy, with over 100 participants and more than 50 organisations represented at the workshop.

The first panel session of the workshop was an opportunity to hear from various stakeholders and from international organisations about significant legal, policy or

technological updates related to privacy & data protection from the perspective of their work.

Moving on to the second panel session of the workshop, participants considered Data Subjects' Rights, specifically the challenges and opportunities for International Organisations. The aim was to get an overview of current best practices and the challenges of enforcing data subjects' rights and discussions included governance, response time and technology used.

The workshop concluded with a session focusing on "Digital Transformation and Data Protection an Oxymoron?", during which participants looked at the tension between innovation and data protection and considered the challenges including anonymisation, role determination, security, data sharing, for instance in AI, cloud computing or Blockchain.

The discussions on both days of the workshop demonstrated the commitment of the international organisations' data protection community. The EDPS will continue to support their efforts and continue to contribute to increasing global cooperation.

The 2020 remote workshop of data protection within International Organisations demonstrated a strong demand on the size of international organisations to have an in-depth discussion with EU's representative on international transfers to international organisations and on practical and pragmatic tools to be developed to facilitate such transfers. A taskforce was established by the EDPS to work further on these questions, in particular on the development of a template administrative arrangement to frame transfers from EUs to international organisations.

G7 Data Protection Authorities (DPAs) roundtable

In 2022, and for the first time ever, the EDPS participated in a Roundtable of G7 DPAs in Bonn, Germany, between 6 and 8 September 2022, at the invitation of the Federal DPA of Germany.

This official event was organised by the Federal DPA of Germany in the context of the German Presidency of the "Group of Seven", an inter-governmental political forum consisting of Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, as well as the European Union. The EU was represented by the EDPS, Wojciech Wiewiorowski, and the Chair of the EDPB.

At the event, the G7 DPAs discussed a wide range of topics, including:

- the "data free flow with trust" concept;
- the intersection of privacy, competition and consumer protection;
- international data transfer tools;
- privacy-enhancing technologies and de-identified data;
- the use of principles of data minimisation and purpose limitation to meet the challenges of commercial surveillance;
- the role of privacy and data protection authorities in the setting and promoting of an ethical and cultural model for the governance of artificial intelligence.

This forum is now established on a more permanent basis and the EDPS is participating to the different working groups created. It is now preparing to participate to the 2023 edition of the G7 DPAs Roundtable that will be organized under the Japanese chairmanship.

2.2 The EDPB in 2022

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules, such as the General Data Protection Regulation 2016/679 (GDPR), throughout the European Economic Area. The EDPB is composed of representatives of the national EU and EEA EFTA data protection supervisory authorities, and the European Data Protection Supervisor (EDPS).

The Secretariat of the EDPB works under the exclusive instructions of the EDPB Chair and is managed by the Head of the EDPB Secretariat. The EDPB Secretariat provides analytical, administrative and logistical support to the EDPB. In practice, the EDPB Secretariat deals with a range of tasks, from drafting EDPB documents, including Art. 65 binding decisions, promoting and supporting enforcement cooperation among Supervisory Authorities (SAs), providing IT solutions to ensuring transparent communications, handling media relations, ensuring respect of the legal framework and planning as well as organising meetings. The EDPB Secretariat is composed of a multifaceted team facilitating the Board's fair and effective decision-making and acts as the gateway for clear and consistent communications.

2.2.1. EDPB 2022 Highlights

A. Enforcement cooperation

The EDPB plays a key role in enforcing data protection laws. It ensures consistent enforcement and promotes enforcement cooperation amongst SAs. In addition, for a small number of complex cases on which SAs cannot agree via consensus, the EDPB takes binding decisions.

Since the General Data Protection Regulation (GDPR) started applying, the EDPB has focused attention and effort on ensuring consistent enforcement based on cooperation. Following the vision laid down in its [2021-2023 Strategy](#), this continues to be a high priority for the EDPB. In that respect, in 2022, the EDPB's work on enforcement cooperation shifted into a higher gear, particularly through the numerous initiatives taken to streamline enforcement cooperation among SAs.

It is worth highlighting the following initiatives:

- A number of taskforces have worked on key topics with a cross-border dimension. This has led to a consistent approach by the SAs on topics such as Google Analytics and cookie banners.
- Following the creation of the Coordinated Enforcement Framework in 2021 for simultaneous and coordinated enforcement actions by SAs, in 2022, 22 SAs undertook coordinated investigations into around 100 cloud services used in the public sector throughout the European Economic Area (EEA).
- For supporting and increasing SAs' capacity to supervise, investigate and enforce, the EDPB launched a [Support Pool of Experts](#) with specialists in various areas, including IT auditing, security and data science.

All these efforts contribute to better internal work processes, unified strategies, enhanced cooperation and overall streamlining of the enforcement.

Vienna statement on enforcement cooperation

In pursuit of developing a comprehensive and collaborative approach to address issues related to GDPR enforcement, the EDPB Members met in Vienna in April 2022 and reiterated their commitment to close cross-border cooperation. A statement summarised the Members' agreed action towards strong and swift enforcement of the GDPR through further enhancing cooperation on strategic cases and diversifying the range of cooperation methods used. Among other topics, the EDPB agreed to identify a list of procedural aspects that could be further harmonised in EU law to maximise the positive impact of GDPR cooperation. This list was sent to the EC for its consideration in October 2022, and was added to the EC's 2023 work programme.

Going forward, the EDPB will also prioritise enforcement actions by fostering greater cooperation on cross-border cases of strategic importance, addressing legal challenges stemming from matters of general application, and better aligning national enforcement strategies.

Guidelines 02/2022 on Art. 60 GDPR

In line with the broader narrative to support effective enforcement and efficient cooperation between national SAs, the EDPB adopted Guidelines 02/2022 focusing on the interactions of SAs with each other, the EDPB and third parties under Art. 60 GDPR. The aim is to provide guidance in terms of cooperation and the One-Stop-Shop (OSS) mechanism. In practice, this helps SAs to enact their own national procedures in a manner consistent with the cooperation under the OSS mechanism.

The guidelines elaborate and clarify the requirements of each paragraph of Art. 60 GDPR, based on the provision's text and its practical implementation. Overall, the provided clarification and guidance of the requirements under Art. 60 GDPR significantly contribute to the desired consistency of the SAs' work and in enhancing enforcement cooperation.

Guidelines 04/2022 on the calculation of fines

To harmonise the approach used by SAs in calculating fines, the EDPB adopted the first version of Guidelines 04/2022. The guidelines contribute to an important part of the EDPB's strategy in creating more efficient cooperation among SAs on cross-border cases, as they devised a systematic and chronological five-step methodology that SAs across the EEA can use for calculating administrative fines for infringements of the GDPR.

B. Article 65 decisions

The EDPB is empowered to issue binding decisions under Art. 65 GDPR to guarantee the consistent application of the GDPR by SAs. In 2022, the EDPB issued [5 binding decisions](#), leading to a total amount of EUR 801 million in fines, addressing a range of issues from right to access, right to object direct marketing, protection of children's use of social media to legal basis for processing personal data.

Decision 01/2022³⁴ on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Art. 65(1)(a) GDPR

³⁴ https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/decision-012022-dispute-arisen-draft_en

In June 2022, the EDPB settled a dispute regarding a fine against the French hospitality company Accor SA in its Decision 01/2022.

The French lead supervisory authority (LSA) issued a draft decision against Accor SA following complaints relating to a failure to consider the right to object to the receipt of marketing messages by mail and/or difficulties encountered in exercising the right of access.

The EDPB decided that the French LSA needed to reassess the elements it relied upon to calculate the amount of the fine for ensuring that it meets the criterion of dissuasiveness. The EDPB clarified that the fine should be determined solely based on the company's turnover of the preceding year, namely 2021, without considering the reduced turnover caused by the COVID-19 pandemic as a mitigating factor under 83(2)(k) GDPR.

The fine issued to Accor was increased from the initial EUR 100 000 imposed by the French LSA to EUR 600 000 following the EDPB's binding decision.

Binding Decision 02/2022³⁵ on the dispute arisen on the draft decision of the Irish SA regarding Meta Platforms Ireland Limited (Instagram) under Art. 65(1)(a) GDPR

In July 2022, the EDPB adopted a binding decision regarding Instagram (Meta IE), particularly on the policy of maintaining public-by-default profiles of children and the mandatory public disclosure of their contact details when operating business accounts.

The Irish LSA triggered the dispute resolution procedure under Art. 65 GDPR after no consensus had been reached on the objections raised by several other SAs concerned (CSAs) with regard to the legal basis for processing and the determination of the fine.

In terms of publicly disclosing children's contact details when they operate business accounts, Meta IE relied on two legal bases for processing personal data: "performance of a contract" and "legitimate interests". The EDPB found that Meta IE could not have relied on performance of a contract as a legal basis for the publication since the processing at stake was not necessary for the performance of a contract between Meta IE and its child users. Regarding legitimate interests, the EDPB concluded that the publication of the children's contact details did not meet the requirements because the processing was either unnecessary or, if it were to be considered necessary, it did not pass the balancing test required when determining legitimate interests.

Therefore, the EDPB concluded that Meta IE unlawfully processed children's personal data and it further instructed the Irish LSA to amend its draft decision by including the infringement of Art. 6(1) GDPR.

The EDPB also instructed the Irish SA to assess its envisaged administrative fine in accordance with Art. 83(1)-(2) GDPR.

On the issue of public-by-default profiles of children, the Irish SA was not required to amend its draft decision. Indeed, the EDPB concluded that the objection did not meet the requirements of being "relevant and reasoned" under Art. 4(24) GDPR.

³⁵ https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22022-dispute-arisen_en

Following the EDPB's binding decision, the Irish LSA adopted its final decision against Meta IE. They determined that Meta IE had infringed Art. 6(1) GDPR. The final fine was EUR 405 million.

Binding Decision 3/2022 on the dispute submitted by the Irish Supervisory Authority (SA) on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR) and Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)

Following the EDPB's [binding dispute resolution decisions](#) of 5 December 2022, the Irish SA (IE SA) adopted its decisions regarding Facebook and Instagram (Meta IEv). These decisions are the result of complaint-based inquiries into Facebook's and Instagram's activities in particular concerning the lawfulness and transparency of processing for behavioural advertising.

The binding decisions were adopted on the basis of Art. 65(1)(a) GDPR, after the IE SA as LSA had triggered two dispute resolution procedures concerning the objections raised by CSAs from ten countries in each case. Among others, CSAs issued objections concerning the legal basis for processing (Art. 6 GDPR), data protection principles (Art. 5 GDPR), and the use of corrective measures including fines.

The EDPB decided that Meta IE inappropriately relied on contract as a legal basis to process personal data in the context of Facebook's Terms of Service and Instagram's Terms of Use for the purpose of behavioural advertising as this was not a core element of the services. The EDPB found in both cases that Meta IE lacked a legal basis for this processing and therefore unlawfully processed these data. As a consequence, the EDPB instructed the IE SA to amend the finding in its draft decisions and to include an infringement of Art. 6(1) GDPR.

The EDPB instructed the IE SA to include, in its final decisions, an order for Meta IE to bring its processing of personal data for behavioural advertising in the context of the Facebook and Instagram services into compliance with Art. 6(1) GDPR within three months.

Next, the EDPB examined whether the complaints had been addressed with due diligence. The complainant had raised the fact that sensitive data is processed by Meta IE. However, the IE SA did not assess processing of sensitive data and therefore, the EDPB did not have sufficient factual evidence to enable it to make findings on any possible infringement of the controller's obligations under Art. 9 GDPR. As a result, the EDPB disagreed with the IE SA's proposed conclusion that Meta IE is not legally obliged to rely on consent to carry out the processing activities involved in the delivery of its Facebook and Instagram services, as this could not be categorically concluded without further investigations. Therefore, the EDPB decided that the IE SA must carry out a new investigation.

In addition, the EDPB instructed the IE SA to include in both final decisions a finding of infringement of the principle of fairness and to adopt the appropriate corrective measures. The EDPB noted that the grave breaches of transparency obligations impacted the reasonable expectations of the users, that Meta IE had presented its services to users in a misleading manner, and that the relationship between Meta IE and users was imbalanced.

With respect to the administrative fines, the EDPB directed the IE SA to impose an administrative fine for the additional infringements of Article 6(1) GDPR (lack of legal basis for the processing of personal data) and to issue significantly higher fines for the transparency infringements identified, as it found the fines proposed did not fulfil the requirement of being effective, proportionate and dissuasive. This led to the IE SA significantly increasing the fines in its final decisions (from a maximum of EUR 36 million and EUR 23 million for the Facebook and Instagram draft decisions, to EUR 210 million and EUR 180 million in the final decisions respectively).

Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR)

Following the EDPB's binding dispute resolution decision of 5 December, WhatsApp IE was issued a EUR 5.5 million fine by the Irish SA (IE SA).

In its Binding Decision, the EDPB instructed the IE SA to amend its draft decision with respect to the findings concerning lawfulness of the processing and the principle of fairness, and to the corrective measures envisaged.

Regarding the lawfulness of processing for service improvement purposes, the EDPB decided that WhatsApp IE inappropriately relied on contract as a legal basis to process personal data. As a consequence, the EDPB instructed the IE DPSAA to add an infringement of Art. 6(1) GDPR. Additionally, the EDPB instructed the IE SA to include an infringement of the principle of fairness under Art. 5(1)(a) GDPR.

The EDPB further decided that the IE SA must carry out an investigation into WhatsApp IE's processing operations in order to determine whether it processes special categories of personal data (Art. 9 GDPR); whether it processes data for the purposes of behavioural advertising, for marketing purposes, as well as for the provision of metrics to third parties and the exchange of data with affiliated companies for the purposes of service improvements.

With respect to corrective measures, the EDPB requested the IE SA to include in its final decision an order for WhatsApp IE to bring its processing of personal data for the purposes of service improvement in the context of its Terms of Service into compliance with Art. 6(1) GDPR within a specified period of time, and to cover the infringements of Art. 6(1) GDPR with an administrative fine.

2.2.2. Meetings

In 2022, the EPDB Secretariat organised 347 meetings for the EDPB, including 15 plenary meetings, 160 expert subgroup or taskforce meetings and 172 drafting teams. One significant distinction from previous years is that in 2022, the EDPB convened hybrid meetings for the first time. Out of 347 meetings, 34 were hybrid, whereas 308 were held remotely and five took place in-person.

During these meetings the EDPB members formally adopted documents or discussed developments or policy questions in relation to issues of significant strategic importance.

The EDPB Secretariat takes part in all of those meetings, provides analytical support and makes all the administrative arrangements.

2.2.3. Guidelines, Opinions, Decisions and other documents

During the plenary meetings, the EDPB adopted Guidelines, Opinions, Decisions and other documents such as statements or informative notes to advise the EC, national SAs, and other stakeholders on GDPR matters.

The EDPB Secretariat led the drafting of 26 opinions, binding decisions and statements adopted by the EDPB in 2022 and contributed to further 23 guidelines, opinions, binding decisions, statements and recommendations.

2.2.3.1. Guidelines

In 2022, the EDPB adopted eight new guidelines and one set of recommendations aimed at clarifying the range of provisions under the GDPR.

- [Guidelines 02/2022 on the application of Article 60 GDPR](#)
- [Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them](#)
- [Guidelines 04/2022 on the calculation of administrative fines under the GDPR](#)
- [Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement](#)
- [Guidelines 06/2022 on the practical implementation of amicable settlements](#)
- [Guidelines 07/2022 on certification as a tool for transfers](#)
- [Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority](#)
- [Guidelines 9/2022 on personal data breach notification under GDPR](#)
- [Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules \(Art. 47 GDPR\)](#)

2.2.3.2. Consistency opinions

Opinions on draft decisions regarding Binding Corporate Rules

SAs may approve Binding Corporate Rules (BCRs) within the meaning of Art. 47 GDPR.

BCRs are data protection policies implemented and adhered to within a group of enterprises established in the EEA for transfers of personal data outside the EEA within the same group. In 2022, several SAs submitted their draft decisions regarding the controller or processor BCRs of various companies to the EDPB, requesting an opinion under Art. 64(1)(f) GDPR. The EDPB issued 23 opinions on BCRs.

In all instances, the EDPB concluded that the draft BCRs contained all required elements and guaranteed appropriate safeguards to ensure that the level of protection ensured by the GDPR would not be undermined when personal data was transferred to and processed by the group members based in third countries. It is without prejudice to the obligation of the data exporter to assess whether, in the specific case, additional measures are necessary to ensure an essentially equivalent level of protection as that provided in the EU. In every case, based on the EDPB opinions, the BCRs could be approved without changes by the relevant SAs.

The various opinions are listed below:

- [Opinion 02/2022 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the WEBHELP Group Adopted: 7 February 2022;](#)

- [Opinion 03/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the WEBHELP Group Adopted: 7 February 2022;](#)
- [Opinion 04/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Norican Group Adopted: 18 March 2022;](#)
- [Opinion 05/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Lundbeck Group Adopted: 19 April 2022;](#)
- [Opinion 06/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Groupon International Limited Adopted: 19 April 2022;](#)
- [Opinion 07/2022 on the draft decision of the Hungarian Supervisory Authority regarding the Controller Binding Corporate Rules of MOL Group Adopted: 19 April 2022;](#)
- [Opinion 08/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Bioclinica Group Adopted: 4 May 2022;](#)
- [Opinion 09/2022 on the draft decision of the Danish Supervisory Authority regarding the Processor Binding Corporate Rules of Bioclinica Group Adopted: 4 May 2022;](#)
- [Opinion 10/2022 on the draft decision of the Hesse Supervisory Authority \(Germany\) regarding the Controller Binding Corporate Rules of Fresenius Group Adopted: 16 June 2022;](#)
- [Opinion 17/2022 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the ANTOLIN Group Adopted: 1 August 2022;](#)
- [Opinion 18/2022 on the draft decision of the Baden-Württemberg \(Germany\) Supervisory Authority regarding the Controller Binding Corporate Rules of the Daimler Truck Group Adopted: 26 August 2022;](#)
- [Opinion 19/2022 on the draft decision of the Baden-Württemberg \(Germany\) Supervisory Authority regarding the Controller Binding Corporate Rules of the Mercedes-Benz Group Adopted: 26 August 2022;](#)
- [Opinion 20/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ellucian Group Adopted: 26 August 2022;](#)
- [Opinion 21/2022 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Ellucian Group Adopted: 26 August 2022;](#)
- [Opinion 22/2022 on the draft decision of the Liechtenstein Supervisory Authority regarding the Controller Binding Corporate Rules of Hilti Group Adopted: 7 September 2022;](#)
- [Opinion 23/2022 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of the Samres Group Adopted: 7 September 2022;](#)
- [Opinion 24/2022 on the draft decision of the Swedish Supervisory Authority regarding the Processor Binding Corporate Rules of the Samres Group Adopted: 7 September 2022;](#)

- [Opinion 26/2022 on the draft decision of the Data Protection Authority of Bavaria for the Private Sector regarding the Controller Binding Corporate Rules of the Munich Re Reinsurance Group Adopted: 30 September 2022;](#)
- Opinion 27/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of LEYTON Group Adopted: 7 October 2022.
- Opinion 29/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the DSV Group Adopted: 18 November 2022
- Opinion 30/2022 on the draft decision of the Slovak Supervisory Authority regarding the Controller Binding Corporate Rules of the Piano Group Adopted on 28/11/2022
- Opinion 31/2022 on the draft decision of the Slovak Supervisory Authority regarding the Processor Binding Corporate Rules of the Piano Group Adopted on 28/11/2022
- Opinion 32/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ramboll Group Adopted on 06/12/2022

Opinions on draft requirements for accreditation of a certification body

Three SAs submitted their draft decisions on accreditation requirements for certification bodies under Art. 43(1)(b) GDPR to the EDPB, requesting an opinion under Art. 64(1)(c) GDPR. These requirements allow the accreditation of certification bodies responsible for issuing and renewing certification in accordance with Art. 42 GDPR.

These opinions aim to establish a consistent and harmonised approach regarding the requirements that SAs and national accreditation bodies apply when accrediting certification bodies under the GDPR. To do so, the EDPB made recommendations to the relevant SAs on the amendments to be made to the draft accreditation requirements. The SAs then amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the opinions of the EDPB.

The various opinions are listed below:

- [Opinion 11/2022 on the draft decision of the competent Supervisory Authority of Poland regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted: 4 July 2022;](#)
- [Opinion 12/2022 on the draft decision of the competent Supervisory Authority of France regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted: 4 July 2022;](#)
- [Opinion 13/2022 on the draft decision of the competent Supervisory Authority of Bulgaria regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 \(GDPR\) Adopted: 4 July 2022.](#)

Opinions on certification criteria

When an SA intends to approve a certification pursuant to Art. 42(5) GDPR, the main role of the EDPB is to ensure the consistent application of the GDPR through the consistency mechanism referred to in Arts. 63, 64 and 65 GDPR. Under this framework, according to Art. 64(1)(c) GDPR, the EDPB is required to issue an opinion on an SA's draft decision approving the certification criteria. The EDPB issued two opinions on certification criteria in 2022, aiming at ensuring the consistent application of the GDPR, including by the SAs, controllers and processors.

The two opinions are listed below:

- [Opinion 01/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria Adopted: 8 February 2022;](#)
- [Opinion 25/2022 regarding the European Privacy Seal \(EuroPriSe\) certification criteria for the certification of processing operations by processors Adopted: 22 September 2022.](#)

Opinions on SAs’ approval of accreditation requirements for code of conduct monitoring body

In 2022, The EDPB issued three opinions on draft accreditation requirements for code of conduct monitoring bodies, as requested by SAs in accordance with Art. 64(1)(c) GDPR.

The aim of these EDPB opinions is to ensure consistency and the correct application of the requirements among SAs. To do so, the EDPB made several recommendations to the various SAs on the amendments to be made to the draft accreditation requirements. On this basis, the SAs amended their drafts in accordance with Art. 64(7) GDPR, taking utmost account of the opinions of the EDPB.

The various Opinions are listed below:

- [Opinion 14/2022 on the draft decision of the competent Supervisory Authority of Bulgaria regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR Adopted: 4 July 2022;](#)
- [Opinion 15/2022 on the draft decision of the competent Supervisory Authority of Luxembourg regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR Adopted: 4 July 2022;](#)
- [Opinion 16/2022 on the draft decision of the competent Supervisory Authority of Slovenia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to Art. 41 GDPR Adopted: 4 July 2022.](#)

2.2.3.3. Other documents, including legal advice

The following documents were adopted in 2022:

EDPS-EDPB Joint opinion 01/2022 on Covid-19 certification Regulation extension

On 3 February 2022, the EC adopted, firstly, a [Proposal for a Regulation on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates \(EU Digital COVID Certificate\) to facilitate free movement during the COVID-19 pandemic](#) for EU citizens, and secondly, a [Proposal for a Regulation](#) on the same matters, but applying to third-country nationals legally staying or residing in the territories of Member States.

As a general remark, the EDPB and the EDPS recalls that compliance with data protection rules does not constitute an obstacle to fighting the COVID-19 pandemic and that, at the same time, the general principles of effectiveness, necessity and proportionality must guide any measure adopted by Member States or EU institutions that involve processing personal data to fight COVID-19. In addition, the EDPB and the EDPS underlined that any restriction to the free movement of persons within the European Union put in place to limit the spread of SARS-CoV-2, including the requirement to present EU Digital COVID Certificates, should be lifted as soon as the epidemiological situation allows.

The EDPS and EDPB took note that the EC did not carry out an impact assessment for the Proposals, due to the urgency and their limited scope. They strongly considered that the Proposals should be accompanied by an impact assessment report, for providing a clear justification on the necessity and proportionality, taking into account the evolution of the epidemiological situation with regard to the COVID-19 pandemic together with the impact on fundamental rights and non-discrimination.

Lastly, the EDPB and the EDPS invites the EC to assist the Member States in developing technical specifications on the recognition of information about the COVID-19 vaccine and the number of doses administered to the holder, regardless of the Member State in which they have been administered.

EDPB-EDPS Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

In a joint effort, the EDPB and the EDPS comments on overarching concerns related to the [Proposal on Data Act](#) and urges the co-legislator to take decisive action. While welcoming the efforts made to ensure that the Proposal does not affect the current data protection framework, the EDPB and the EDPS consider that additional safeguards are necessary to avoid lowering the protection of the fundamental rights to privacy and to the protection of personal data in practice. Their comments concern three distinct areas: i) the rights to access, use and share data, ii) the obligation to make data available in case of “exceptional need”, and iii) the implementation and enforcement.

First, the Joint Opinion stresses the need for provisions explicitly specifying that data protection law “prevails” in case of conflict with the provisions of the Proposal insofar as the processing of personal data is concerned. In addition, a more robust application of the data minimisation principle is encouraged when designing new products. Along with that, the Opinion calls for an enhancement of the right to data portability. In general, the EDPB and the EDPS stresses the need to ensure that access, use, and sharing of personal data by users other than data subjects, as well as by third parties and data holders, should occur in full compliance with all of the provisions of the GDPR, EUDPR and ePrivacy Directive.

Second, the EDPB and the EDPS expresses concerns regarding the lawfulness, necessity and proportionality of the obligation to make data available to public sector bodies and EU institutions, agencies or bodies in case of “exceptional need”. They reminded that any limitation on the right to personal data protection must be based on a legal basis that is adequately accessible and foreseeable and formulated with sufficient precision to enable individuals to understand its scope.

Third, regarding implementation and enforcement, the EDPB and the EDPS highlights the risk of operational difficulties that might result from the designation of more than one competent authority responsible for the application and enforcement of the Proposal. At the same time, they welcomed the designation of the data protection SAs as competent authorities responsible for monitoring the application of the Proposal insofar as the protection of personal data is concerned. they ask the co-legislators to also designate national data protection SAs as coordinating competent authorities under this Proposal.

EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space

The EDPB and the EDPS jointly expressed their views on the proposed [Regulation on the European Health Data Space](#). The resulting opinion first notes that the Proposal aims at: i) supporting individuals to take control of their own health data, ii) supporting the use of health data for better healthcare delivery, better research, innovation and policy making, and iii) enabling the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data. However, they are concerned that the Proposal may weaken the protection of the rights to privacy and to data protection, especially considering the categories of personal data and purposes that are related to the secondary use of data. They also note that the Proposal will add yet another layer to the already complex (multi-layered) collection of provisions (to be found both in the EU and Member States law) on the processing of health data (in the health care sector). In that respect, the EDPB and the EDPS consider that it is important to clarify the relationship between the provisions in the Proposal with the ones in the GDPR and Member State laws. Additionally, with regards to the scope, they recommend excluding wellness applications and other digital applications, as well as wellness and behaviour data relevant to health. Should this be maintained, the EDPB and the EDPS suggest that personal data deriving from wellness apps and other digital health applications should not be included in the secondary use of health data, as they do not have the same data quality requirements and characteristics as those generated by medical devices. Further, they strongly recommend not extending the scope of the GDPR exceptions regarding the data subject's rights and note the need to remain consistent with the relevant GDPR provisions.

The EDPB and the EDPS suggest that personal data deriving from wellness apps and other digital health applications should not be included in the secondary use of health data, as they do not have the same data quality requirements and characteristics as those generated by medical devices. The EDPB and the EDPS are of the view that the Proposal should further delineate these purposes for secondary use and circumscribe when there is a sufficient connection with public health and/or social security. Lastly, the EDPB and the EDPS acknowledge that the infrastructure for the exchange of electronic health data foreseen in the Proposal will not establish a central EU-database of health data and will only facilitate the exchange of such health data from decentralised databases. However, due to the large quantity of data that would be processed and their highly sensitive nature, among others, the EDPB and the EDPS call for a requirement for storing the personal electronic health data in the EU/EEA, without prejudice to further transfers in compliance with Chapter V of the GDPR.

EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse

In relation to the EC's [Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse](#), the EDPB and the EDPS adopted a joint opinion on 28 July 2022. While emphasizing the gravity of child sexual abuse as a serious and heinous crime, the opinion expresses serious concerns regarding the proportionality of the envisaged interference and limitations to the protection of the fundamental rights to privacy and the protection of personal data.

The EDPB and EDPS note that the Proposal's lack of detail, clarity, and precision regarding the conditions for issuing a detection order for child sexual abuse material (CSAM) and child solicitation does not ensure that only targeted approaches to detecting CSAM are used. They raise the concern that the Proposal could potentially be used as a basis for generalised and indiscriminate scanning of the content of all types of electronic communications. As a result, the EDPB and EDPS recommend that the conditions for issuing detection orders be further clarified to address these concerns.

Additionally, the EDPB and EDPS raise concerns about the measures envisaged for the detection of unknown CSAM and the solicitation of children in interpersonal communication services, in particular due to the likelihood of errors and their high level of intrusiveness into the privacy of individuals. Overall, the EDPB and the EDPS argue that the requirement imposed on online service providers to decrypt online communications in order to block those related to CSAM is disproportionate to the aim pursued.

The EDPB and EDPS underline that breaking or weakening encryption for accessing private communications would have a substantial impact on the right to private life and to the confidentiality of communications, freedom of expression, innovation and growth of the digital economy.

Lastly, the EDPB and EDPS recommend that the relationship between the tasks of the national Coordinating Authorities under the Proposal and SAs be better regulated. They also underline that the transmission of personal data between the newly proposed EU Centre and Europol should only take place following a duly assessed request case-by-case.

Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework

The GDPR requires that the EC seeks an opinion of the EDPB before adopting a possible new adequacy decision recognising as satisfactory the level of data protection guaranteed by a third country. In principle, the EDPB welcomes the announcement of a political agreement between the European Commission and the United States (U.S.) on 25 March 2022 on a new Trans-Atlantic Data Privacy Framework. This announcement is made at a time when transfers from the EEA to the U.S. face significant challenges.

The EDPB looks forward to carefully assessing the improvements that a new Trans-Atlantic Data Privacy Framework may bring in light of the EU law, the case law of the CJEU and the recommendations EDPB made on that basis. In particular, the EDPB will analyse in detail how these reforms ensure that the collection of personal data for national security purposes is limited to what is strictly necessary and proportionate.

Lastly, the EDPB will examine to what extent the announced independent redress mechanism respects the EEA individuals' right to an effective remedy and to a fair trial. In particular, the EDPB will look at whether any new authority involved in this mechanism has access to relevant information, including personal data, when exercising its mission and can adopt decisions binding on the intelligence services, and whether there is a judicial remedy against this authority's decisions or inaction.

Response of the EDPB to the European Commission's targeted consultation on a digital Euro

In April 2022, the EC launched a public consultation to gather information on the expected impact of the digital euro on stakeholders, including with regard to its privacy and data protection aspects.

In its contribution to this consultation, the EDPB recalls the views it expressed to the EUIs in a letter of June 2021, namely that a high level of data protection and privacy rights is crucial to strengthen end-users' trust in the digital euro project, and thus to ensure its acceptance by European citizens. For achieving this, the EDPB recommends that the features of the digital euro be designed as closely as possible to physical cash.

In particular, the EDPB stresses the importance of providing individuals with a bearer-based architecture available both online and offline. Furthermore, the EDPB is of the opinion that controls of transactions should only be carried out by the competent authorities and reduced to the minimum necessary. Finally, the EDPB recommends that such transactions should not be traceable at all below a certain threshold.

Other Guidance and Information Notes:

Statement 02/2022³⁶ on personal data transfers to the Russian Federation

Recent geopolitical developments had Russia excluded from the CoE on 16 March 2022. Although Russia continues to be a contracting party to conventions and protocols concluded in the framework of the CoE to which it has expressed its consent to be bound, for instance, Convention 108, the modalities of Russia's participation in these instruments are still to be determined.

In its Statement, the EDPB recalls that the transfer of personal data to a third country, in the absence of an adequacy decision of the EC pursuant to Art. 45 GDPR, is only possible if the controller or processor has provided appropriate safeguards, and on condition that enforceable rights and effective legal remedies are available for data subjects (Art. 46 GDPR), or in specific circumstances, only on one of the conditions set forth in Art. 49 GDPR.

Russia does not benefit from an adequacy finding by the EC in accordance with Art. 45 GDPR. Therefore, the EDPB notes that, when personal data are transferred to Russia, data exporters under the GDPR should assess and identify the legal basis for the transfer and the instrument to be used among those provided by Chapter V GDPR (e.g., Standard Contractual Clauses or Binding Corporate Rules), in order to ensure the application of appropriate safeguards.

SAs of EEA Member States which have close economic and historic ties with Russia are already looking into the lawfulness of data transfers to Russia, including in the context of ongoing investigations. They will handle cases involving data transfers to Russia, taking into account the increased impact on the rights and freedoms of data subjects that may arise from such data processing operations, and will coordinate within the EDPB, as appropriate.

³⁶ https://edpb.europa.eu/our-work-tools/our-documents/other/statement-022022-personal-data-transfers-russian-federation_en

Statement on enforcement cooperation

On 28 April 2022, the EDPB adopted a [Statement on enforcement cooperation](#), following a high-level meeting in Vienna where EDPB members agreed to enhance cooperation on strategic cases and to diversify the range of cooperation methods used.

The statement recalls the SAs' commitment to close cross-border cooperation. The SAs agreed to collectively and regularly identify cross-border cases of strategic importance, with the EDPB's support, in different Member States. Additionally, SAs committed to further exchange information on national enforcement strategies for reaching an agreement on annual enforcement priorities at the EDPB level.

The Statement also reiterates the EDPB's role in ensuring a consistent interpretation of the GDPR. The EDPB shall deal with specific legal issues on matters of general application as well as facilitate the cross-border exchange of information. Lastly, for maximising the positive impact of GDPR cooperation, the EDPB will identify a list of procedural aspects that can be further harmonised in EU law.

Statement 04/2022 on the design choices for a digital euro from the privacy and data protection perspective

In its Statement, the EDPB emphasises the importance of ensuring a very high standard of privacy and data protection by design and by default in the digital euro project. To meet this standard, the EDPB suggests that different design choices should be considered and adopted based on a documented impact assessment prioritising innovative and privacy-enhancing technologies.

The EDPB cautions against the use of systematic validation and tracing of all transactions in digital euro. In this regard, the EDPB advises that the digital euro be made available both online and offline, along a threshold below which no tracing is possible, for guaranteeing full anonymity of daily transactions.

The EDPB also welcomes the EC's intention to propose in 2023 a specific legal framework for the digital euro, for which it stands ready to provide relevant guidance. Finally, the EDPB urges the ECB and the EC to enhance public debate on the digital euro project to ensure it meets the highest standards of privacy and data protection.

EDPB Document on the selection of cases of strategic importance

Following the Vienna meeting of April 2022, the EDPB adopted a document that establishes criteria for determining whether a case is of strategic importance, in line with the [Statement on enforcement cooperation](#). The EDPB considers cases to be of strategic importance if there is a high risk to the rights and freedoms of natural persons in several Member States.

Pursuant to the document, a proposal voluntarily submitted by an SA may qualify as a case of strategic importance if it concerns a structural or recurring problem in several Member States, is related to the intersection of data protection with other legal fields, and/or affects a large number of data subjects in several Member States. Cases that involve a large number of complaints in several Member States, a fundamental issue falling within the scope of the EDPB strategy, and/or matters where the GDPR implies that high risk can be assumed, also qualify as strategically important cases.

Further, the EDPB lays down in its document the process and timeline for the selection of cases. A template for the proposal of a strategic case is also provided by the EDPB, to ensure that Member States include all the information relevant to the case when submitting their proposal.

2.2.4. Stakeholder engagement

The EDPB organises stakeholder events to gather input and views on specific issues in the interest of developing future guidance. In September 2022, the EDPB organised an event with a series of non-governmental organisations. The meeting topic was the EDPB's actions on GDPR enforcement, following the Commissioner's meeting in Vienna, including the identification of procedural aspects to be harmonised in EU law. The participating NGOs contributed on the following issues:

- lodging of complaints with SAs;
- procedural deadlines;
- access to files;
- the right to be heard;
- legal remedies.

Following the preliminary adoption of guidelines, the EDPB Secretariat organises public consultations to give stakeholders and citizens the opportunity for additional input. This input is then taken into account by the EDPB members in charge of drafting.

In 2022, the EDPB Secretariat was consulted on the following documents:

- [Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules \(Art. 47 GDPR\)](#)
- [Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority](#)
- [Guidelines 9/2022 on personal data breach notification under GDPR](#)
- [Guidelines 07/2022 on certification as a tool for transfers](#)
- [Guidelines 04/2022 on the calculation of administrative fines under the GDPR](#)
- [Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement](#)
- [Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them](#)
- [Guidelines 01/2022 on data subject rights - Right of access](#)

For the fourth year in a row, the EDPB Secretariat conducted a survey as part of the annual review of the Board's activities under Article 71.2 GDPR. Questions focused on the content and adoption process of the EDPB's Guidelines, with a view to understanding to what extent stakeholders find them helpful and practical to interpret GDPR's provisions.

2.2.5. The EDPB Secretariat contribution to the national SAs' cooperation

As part of its 2021-2023 Strategy, the EDPB established a Support Pool of Experts (SPE) in 2020. The SPE's main objective, is to assist SAs in carrying out investigations and enforcement activities of significant common interest. The SPE provides support in the form of expertise for investigations and enforcement activities of common interest

to SAs and enhances cooperation/solidarity by reinforcing and complementing the strengths of the individual SAs and addressing operational needs. This includes but is not limited to, analytical support, assistance in the performance findings of a forensic nature, as well as in the preparation of investigative reports on the basis of evidence collected. Further, the SPE enhances the cooperation and solidarity between all EDPB members by sharing, reinforcing and complementing strengths and addressing operational needs.

A call for external experts was launched and at the end of 2022, the SPE was composed of 409 external experts. Further in line with the 2021-2023 Strategy, the EDPB set up a [Coordinated Enforcement Framework](#) (CEF). The CEF provides a structure for recurring annual coordinated action by the SAs. The CEF aims to facilitate joint actions in a flexible and coordinated manner, ranging from joint awareness raising and information gathering to enforcement sweeps and joint investigations. The purpose behind the recurring annual coordinated actions is to promote compliance, empower data subjects to exercise their rights and raise awareness.

The EDPB's first joint action under the CEF focused on the use of cloud-based services by the public sector. 22 SAs took part and launched coordinated investigations. In its final report on CEF 2022, the EDPB underlines the need for public bodies to act in full compliance with the GDPR and includes recommendations for public sector organisations when using cloud-based products or services. In addition, a list of actions already taken by data protection authorities in the field of cloud computing is made available.

For 2023, participating DPAs have chosen the topic of the designation and position of data protection officers (DPOs).

The EDPB Secretariat is also in charge of the management of a [register on the EDPB website gathering the final decision taken concerning cross-border cases in the context of the OSS mechanism](#). The register offers an exceptional opportunity to read final decisions taken by, and involving, different SAs in a cross-border context. These decisions often contain useful guidance on how to comply with the GDPR in practice. The register contains both final decisions and its summaries prepared by the EDPB Secretariat and duly approved by LSAs.

2.2.6. IT communications tool (Internal Market Information) & the new EDPB website

In the context of cooperation between SAs, the EDPB Secretariat provides continuous support to SAs with IT solutions that facilitate their communication. In this respect, the EDPB Secretariat leads the IT Users Expert Subgroup, which focuses on the need for development and making changes to the information systems used by EDPB, including the Internal Market Information (IMI) system which is used to exchange information necessary for the GDPR cooperation and consistency mechanism. This included the overhaul of two procedures to reflect the experience gathered in the first years of the GDPR and updates to reflect modifications in the EDPB's Rules of Procedure. In addition, further reporting possibilities were introduced.

Throughout 2022, the EDPB Secretariat continued working on best practices to refine the procedures in use and to share its expertise on the use of the IMI system. While employing the IMI system, the SAs and the EC are supported by the EDPB IMI helpdesk within the EDPB Secretariat. The IMI helpdesk continued to carry out 3 252 proactive monitoring procedures to ensure that case files were complete and registered correctly.

The EDPB Secretariat also performed a follow-up to the migration of the EDPB Wiki platform used for internal sharing of information, with additional functionalities and an enhanced user experience. In addition, the EDPB Secretariat upgraded the case management system (CMS) of the EDPB website '<https://edpb.europa.eu>', which manages the creation and modification of digital content, to Drupal 9. A new advanced search feature to improve the usability of the website was introduced. The EDPB website was visited 275 734 times in 2022. Considerable efforts were made regarding the translation of documents available on the website. In fact, 283 EDPB documents and 159 press releases were translated into 22 languages.

The EDPB Secretariat improved internal tools for the organisation and planning of meetings and for the management of documents.

2.2.7. The EDPB Secretariat activities relating to access to documents

Transparency is a core principle of the EDPB. As an EU body, the EDPB is subject to Art. 15 of the [Treaty of the Functioning of the European Union](#) and [Regulation 1049/2001 on public access to documents](#). Art. 76(2) GDPR and Art. 32 of the EDPB's Rules of Procedure reinforce this requirement. The principle of transparency provides any EU citizen, and any natural or legal person residing or having a registered office in a Member State, with the right of access to EDPB documents. This right applies to all documents held by the EDPB, concerning any matter relating to its responsibilities. In exceptional cases, the EDPB may refuse to disclose all or part of a document. The reasons for such a refusal and corresponding procedural rules are laid down in Regulation 1049/2001 on public access to documents. In 2022, the EDPB received 68 public access requests for documents held by the EDPB. Confirmatory applications were received in seven cases. In accordance with Art. 32(2) of the EDPB Rules of Procedure, the EDPB Secretariat prepares the answers to those requests, which are handled and signed by the Chair of the EDPB (for confirmatory applications) or one of the Deputy Chairs of the EDPB (for initial applications).

Three complaints regarding three EDPB's confirmatory decisions for requests for access to documents, submitted in 2021 and 2022, were brought to the attention of the European Ombudsman in 2022. Whilst the scope of the three complaints varied, their subject matter related to the U.S. Foreign Account Tax Compliance Act and covered draft and final versions of statements, guidelines and letters, as well as correspondence. Following a reassessment of the requested documents, the EDPB decided to grant wider partial access to three documents, which were provided to the complainants.

2.2.8. The EDPB Secretariat activities relating to Data Protection Officer activities

The EDPB processes personal data following [Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data](#) (Regulation 2018/1725). In accordance with Art. 43 of Regulation 2018/1725, the EDPB designated its own DPO team, which is part of the EDPB Secretariat, to handle the processing of personal data. The DPOs position and tasks are defined in Arts. 44 and 45 of Regulation 2018/1725, and are further detailed in the [EDPB DPO Implementing Rules](#).

In 2022, the EDPB, with the assistance of its DPO team, continued to strengthen compliance with Regulation 2018/1725 by enhancing its transparency practices through different means, such as:

- development, publication and update of several privacy notices;
- continued development of several records, as well as publication of a centralised register for records on the EDPB website; and
- addition of new and updated information to its DPO website page.

The DPO team launched internal legal assessments on different issues concerning the EDPB's processing of personal data and identified suitable legal, organisational and, where applicable, technical solutions. The assessments were carried out as part of the DPO's advising function for the EDPB.

In 2022, the DPO team assisted with the handling of data subject requests made on the basis of rights laid out in Art. 17 to Art. 24 of Regulation 2018/1725, individuals requests for information involving the processing of their personal data, and support in handling data breaches under Arts. 34 and 35 of the same Regulation. Two data breaches required a notification to the EDPS.

Additionally, the DPO team delivered various internal training sessions and updated awareness-raising material aimed at EDPB Secretariat staff. These activities were tailored to the needs and expertise of the participants to ensure that all staff members were adequately informed of their responsibilities surrounding personal data processing, but also of their rights as data subjects.

2.2.9. Coordinated Supervision Committee (CSC)

The CSC was created in accordance with Article 62 of [Regulation \(EU\) 2018/1725](#) of 23 October 2018.

Article 62 provides that the EDPS and the national SAs, each acting within the scope of their respective competences, shall cooperate actively to ensure effective supervision of large-scale IT systems and of EUIs. For this purpose, Article 62 sets forth that they shall meet at least twice a year within the framework of the EDPB. This provision allows the EDPB to develop any further working methods as necessary.

Pursuant to Article 62 of Regulation (EU) 2018/1725, the EDPB created the CSC and regulated it in Title VII of the [EDPB Rules of Procedure](#). On that basis, the CSC adopted its own [Rules of Procedure](#) and working methods.

The CSC also conducts its activities in coordinating the supervision of the processing of personal data in an EU large scale IT system or body, office or agency in accordance with the EU legal act establishing the large scale IT system or the EUIs.

IMI System

The CSC ensures coordination in the supervision of the processing of personal data in the Internal Market Information System (IMI) in accordance with Article 21 of Regulation (EU) No 1024/2012 (as modified by Article 38 of [Regulation \(EU\) No 2018/1724](#))

The national SAs of the 27 EU Member States participate in the activities of the CSC in relation to IMI. The national SAs of Iceland, Liechtenstein, and Norway also participate, as their respective countries also apply the EU legal acts governing IMI.

The IMI is a secure, multilingual online tool, developed by the EC in close collaboration with the Member States, that facilitates the exchange of information between public authorities involved in the practical implementation of EU law and helps authorities to

fulfil their cross-border administrative cooperation obligations in multiple Single Market policy areas.

European Union Agency for Criminal Justice Cooperation (Eurojust)

The CSC ensures coordination in the supervision of the processing of operational personal data in the context of cooperation between the national members within Eurojust in accordance with Article 42 (2) of [Regulation \(EU\) No 1727/2018](#).

The national SAs of the 27 EU Member States participate in the activities of the CSC in relation to [Eurojust](#).

European Public Prosecutor's Office (EPPO)

The CSC ensures the coordination in the supervision of the processing of operational personal data in the context of cooperation between the national members within the EPPO in accordance with Article 87 of [Regulation \(EU\) No 1939/2017](#). More information is available on the [EPPO website](#).

The national SAs of the 22 [participating EU Member States](#) participate in the activities of the CSC in relation to the [EPPO](#).

European Union Agency for Law Enforcement Cooperation (Europol)

The CSC ensures that national SAs and the EDPS cooperate closely in their supervision of the processing of personal data transmitted to and from Europol, in accordance with Article 44.2 of [Regulation \(EU\) 2022/991](#).

The national SAs of the 26 [EU Member States](#) that are part of [Europol](#) participate in the activities of the CSC in relation to this EU agency.

Covered in the near future

The processing of personal data in the following EU large scale IT systems and agencies will also fall under the scope of the CSC coordinating activities, once this is foreseen in the EU legal act governing them and they enter into operation.

- The Schengen Information System (SIS)
- Entry/Exit System (EES)
- The European Travel Information and Authorisation System (ETIAS)
- The European Criminal Records Information System on non EU-nationals (ECRIS-TCN)
- Visa Information System (VIS)
- European Asylum Dactyloscopy Database (EURODAC)
- Customs Information System (CIS)
- Interoperability of EES, ETIAS, ECRIS-TCN, EURODAC, SIS, and VIS

Police and Judicial Cooperation:

- Eurojust, the agency responsible for judicial cooperation in criminal matters among EU Member States.
- EPPO, the prosecution agency responsible for investigating, prosecuting and bringing to judgment crimes against the EU budget.

- Europol, the EU law enforcement agency, since the entry into force of the amended Europol Regulation on 28 June 2022

In the future, all coordinated supervision of large EU information systems, bodies, offices and agencies will gradually be moved to the CSC, including:

- Schengen Information System (SIS), ensuring border control cooperation (normally March 2023);
- Entry Exit System (EES), which registers entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Schengen States (expected before the end of 2023);
- European Travel Information and Authorisation System (ETIAS), which tracks visitors from countries who do not need a visa to enter the Schengen Zone (expected in May 2024);
- Visa Information System (VIS), connecting consulates in non-EU countries and all external border-crossing points of Schengen States (expected by the end of 2024);
- Eurodac, which compares fingerprints of asylum applicants to see if they have previously applied for asylum or entered the EU irregularly via another Member State (expected in 2024);
- Customs Information System, which is an automated information system that assists EU State administrative authorities in preventing, investigating and prosecuting operations that are in breach of customs or agricultural legislation.

Police and Judicial Cooperation:

- European Criminal Records Information System on third country nationals (ECRIS-TCN), which allows EU Member State authorities to identify which other Member States hold criminal records on third country nationals or stateless persons being checked (expected for November 2023);

Schengen Information System (SIS) (see above, as this system also fall under Police and Judicial cooperation)

3. Resource management

3.1. The EDPS Ethics Framework Activities

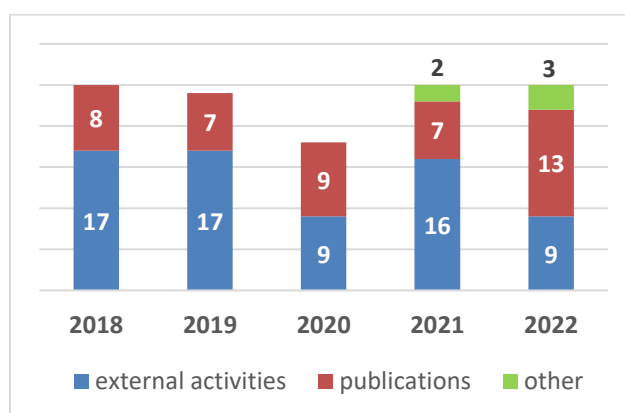
The EDPS policy with regard to professional ethics aims to safeguard the general framework of rights and obligations enshrined in the Staff Regulations and to promote excellence in the European civil service. To guide questions related to professional ethics and staff conduct, the EDPS adopted its own Ethics Framework.

The EDPS Ethics Framework, last updated end of 2019, is composed of a specific Code of conduct for the Supervisor as well as a separate Code of conduct applicable to all staff of the EDPS and the EDPB. These *Codes* of conduct are complemented by a set of decisions on whistleblowing, anti-harassment, disciplinary proceedings and administrative investigations. The appointment of an Ethics officer to the EDPS ensures the compliance with the provisions included in the Framework.

During their induction training, all EDPS and EDPB newcomers attend a mandatory presentation on the Ethics Framework as well as a separate session dedicated to the new anti-harassment decision adopted in 2020. In 2022, two virtual induction trainings were organised for 21 newcomers. Furthermore, a dedicated intranet space provides an additional source of information with guidelines and relevant documents on ethics and staff conduct at the EDPS.

Beginning of 2022, in line with the specific *Code* of conduct for the Supervisor, the Supervisor completed and published his annual declaration of interest. During 2022, the EDPS Ethics officer advised staff on ethical matters and received 25 consultation requests related to the *Code* of conduct for staff, mainly linked to external activities (in particular lectures and presentations) and publications. Following the assessment of the Ethics officer, the Supervisor and the acting Head of the EDPS Secretariat granted authorisations for 16 requests.

Evolution of ethics requests submitted under the EDPS Code of Conduct for all staff



During 2022, no cases of ethical misconduct or whistleblowing were reported the EDPS. Two European Ombudsman cases against the EDPS were closed in 2022 and in 2023 respectively. The first one referred to access to documents and the second one to failure to reply to correspondence on an opinion regarding an administrative enquiry. No maladministration was found. The EDPS was not involved in any OLAF investigation. This can be indeed seen as a very positive indicator for an ethically healthy organisation.

To assess staff's awareness of the EDPS Ethics framework, a related section was included in the staff satisfaction survey launched in June 2022. The survey results confirmed overall reassuring levels of staff awareness regarding professional ethics and also helped pointing to areas that could benefit from reinforcement through targeted trainings. For this purpose, a first session of refresher trainings was organised in November 2022. Additional actions in 2022 included the adoption of an EDPS specific 'patronage policy' in as well as the kick-off for testing the 'on-boarding' of the Commission's Ethics module in Sysper, with a view to introduce an e-workflow for Ethics requests at the EDPS in the course of 2023.

Together with EDPS senior management, the Ethics officer will continue to monitor the implementation of the EDPS Ethics Framework and assess any need for further revision, in particular in the light of the organisational changes and new ways of working induced by the pandemic.

3.2 Human resources

Various data regarding the evolution of the workforce at the EDPS can be found in Annex 2, in particular as regards nationalities, gender, grades and categories of staff. In addition, the EDPS Human Resources, Budget and Administration (HRBA) Unit has been working on different projects during 2022, notably:

3.2.1 Staff working conditions and wellbeing

In May 2022, the significantly improving sanitary situation of the COVID-19 pandemic finally allowed the EDPS to lift the sanitary measures in place and advance in its phased office return strategy by transitioning to a 'new normal' hybrid working mode.

EDPS/EDPB away day

In the aftermath of the pandemic, an EDPS/EDPB staff away day was organised with over 100 participants. This day focused on getting staff back together again after the pandemic, onboarding newcomers and fostering cross team cooperation. The day included many activities and games in a lively and friendly atmosphere.

New hybrid working rules

The HRBA unit prepared a new decision on working arrangements that was adopted in the first half of 2022 together with FAQs explaining the detailed implementation of the decision. The decision aimed to create a hybrid work approach, which combines working from the office and teleworking and helping to promote a modern, flexible working environment, taking into consideration work-life balance. The decision was based on new ways of working learnt throughout the Covid-19 crisis.

Measuring staff satisfaction & follow-up actions:

On a biennial basis, the HRBA Unit invites staff to participate to a Staff Satisfaction Survey (SSS) in order to express their views about work and the workplace. In the 2022 SSS, more than half of the staff (66%) responded to the survey and the results were mostly positive and confirmed a high level of satisfaction and staff engagement at the EDPS.

The HRBA Unit also received some valuable feedback and areas for improvement and therefore, following the results of the 2022 staff satisfaction survey, the EDPS set up a task force for further evaluating the results of the said survey. To do so, HRBA invited each unit and sector to appoint a volunteer to represent them. The task force is self-managed and autonomous therefore, HRBA as a unit does not interfere with the analysis of the results. The task force will share its analysis and recommendations with EDPS staff once completed.

3.2.2 Careers: From recruiting data protection experts to exit interviews

To ensure that the EDPS and EDPB have the personnel and expertise to carry out the tasks assigned to them, there is a need to hire more data protection experts. In order to recruit this workforce, the EDPS organised in 2022, with the support of the European Personnel Selection Office (EPSO), an administrator (AD) specialist open competition that

resulted in the publication of a reserve list of 76 data protection experts, from which the EDPS/EDPB started recruiting as of end of 2022.

Revamped, more candidate-oriented vacancy notices were introduced, aligning them with the EDPS and EDPB employer branding. Once selected and recruited, new staff members can benefit from an enhanced induction programme, to facilitate and speed up their on-boarding.

In May 2022, the HRBA unit finalised the implementation of the paperless management of the probationary period of staff members (STAGE module) in Sysper. The module helps to facilitate the process not only for HRBA but also for managers and staff members. Accordingly, HRBA worked on an update of the guidelines for managers explaining the general procedure to be followed during the probationary period.

In addition, the promotion rules for officials were revised for implementing a fairer system of upgrades, in particular for the ones starting their career as EU officials.

Learning & Development strategy

A learning and development (L&D) strategy sets out the workforce capabilities, skills and competencies the organisation needs, and how they can be developed to ensure a sustainable, successful organisation. The revision of the EDPS L&D strategy was initiated during Q4 2022. The purpose of the revision is to align with the current needs of the EDPS as well as those staff members regarding learning and development. In addition, the EDPS way of working has evolved tremendously since the COVID pandemic; it is thus necessary to ensure that staff learns and is trained in a way which takes advantage of the new learning methods available. The HRBA unit aims to adopt the new strategy by the end of Q1 2023.

EDPB secondment program

The pilot EDPB secondment program – put on hold during the COVID-19 pandemic – was relaunched in 2022. The program applies to the employees (civil servants and contract staff) of all EEA SAs, including the EDPS and EDPB secretariat staff. An assessment of the pilot phase will be carried out in 2023.

Exit interviews

The EDPS adopted its exit interview guidelines in 2022. An exit interview is a wrap-up meeting between the HRBA Head of Unit, a manager and/or a staff committee representative and a staff member who is leaving the institution, either voluntarily or through termination.

Exit interviews are common in the public and private sector. The purpose of the interview is to gather useful feedback that can help guide future practices and improve recruiting and retention.

The specific questions asked in an exit interview vary depending on the type of departure. The exit interview is also an opportunity to provide the staff member with any information they may still require from the institution. At the EDPS, exit interviews are voluntary.

3.2.3 Evolving organisation

During the first semester 2022, the EDPS established an antenna office in Strasbourg. Additionally, in 2022 a reorganisation took place in the EDPS, which resulted in establishing the 'Governance & Internal Compliance' sector (G&IC) and created sub-sectors in S&E for better management of the individual activities. Similar initiatives (creating sub-sectors) were taken by the EDPB, to be rolled out in 2023. The G&IC groups up internal control, data protection, transparency and access to documents as well as archives and records management.

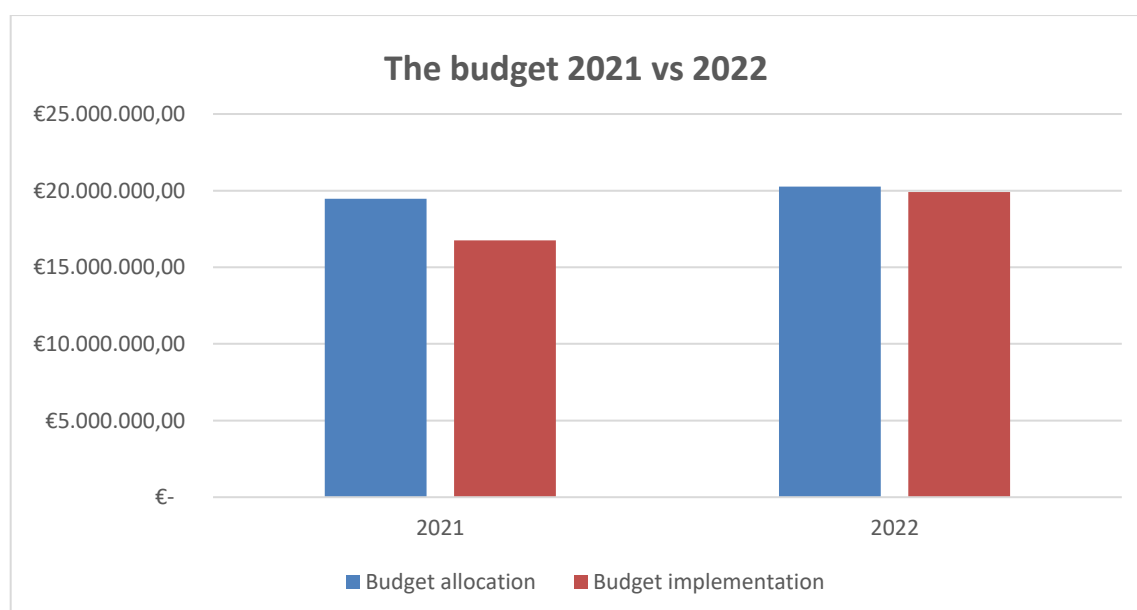
3.3 Budget

3.3.1. Allocated budget for 2022

The 2022 EDPS operating budget amounted to EUR 20 266 000. In addition, EDPS has received EUR 50 000 related to EFTA contribution. Compared to the 2021 final budget, the operating budget increased by 4.12%.

The increase is mainly due to more forecasted expenditures related to Title 1 (staff expenditure) and Title 2 (administrative expenditure).

Other elements impacting the 2022 budget were the consolidation of the EDPB Secretariat (created on 25 May 2018) for which the EDPS was entrusted to provide an independent secretariat and the EDPS strategy 2020-2024 linked to the new mandate.



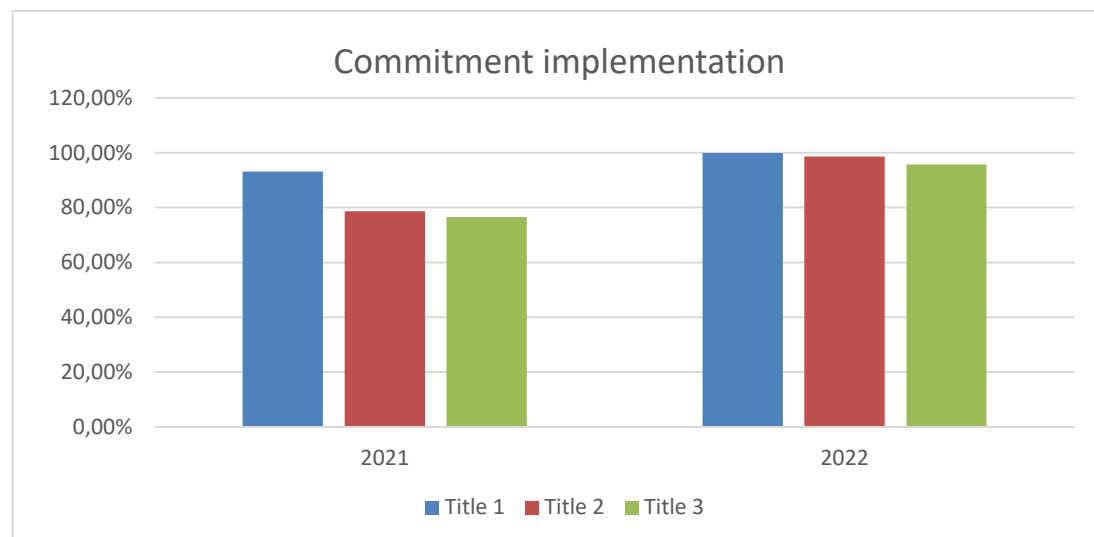
3.3.2. Budget execution 2022

Concerning the overall budget, commitment appropriations show an implementation rate of 98%. This positive trend was made possible through an accurate monitoring of the budget forecast and sound planning of the Institution's activities such as physical events and conferences in presence.

For Title 1, the implementation of commitment appropriations reached 99% also due to a different forecasted annual inflation parameter and unexpected high costs for living. For

Title 2, the commitment implementation rate reached 99%. The implementation rate of the budget line for the experts' reimbursement is 89%, indicates an increase due to the increase of hybrid meetings in 2022.

For Title 3, the implementation rate reached 96%. There was a reduction of the consumption for the budget allocated to the meetings organised by EDPB with the national DPAs and EDPB chair expenses.



3.3.3 Working methods

2022 followed the implementation of *Bluebell*. The EDPS uses *Bluebell* for establishing and revising forecast for the budget based on data uploaded and updated by operational units.

It also enables the EDPS to give a finer view of all budget lines by detailing them into actions (activities) and linking these actions with posting criteria in *ABAC* so that the forecast can be compared in real time with the actual execution.

The implementation of this system increased the efficiency and the monitoring of budget execution. The roll-out of *Bluebell* has generated efficiency gains during the budget preparation and improved the monitoring and the follow-up of the budget implementation. Finally, it has a positive impact for audit trail purposes and ex-post controls.

For the inventory of the EDPS' physical assets, including office equipment, furniture and IT devices, the HRBA unit prepared and conducted the migration to *ABAC Assets*, an accounting system hosted by the EC.

The migration was successfully completed in December 2022 and the new system now allows for considerable efficiency and quality gains for future inventory stocktaking and yearly account closure exercises.

3.3.4 Draft budget 2023 exercise

The 2023 budget exercise, even if very challenging in view of the annual inflation parameters and unexpected high costs of living, was conducted successfully to meet the priorities planned in EDPS.

As was the case in previous budget exercises, the need to follow a rigorous approach in respect of the administrative expenditure and staffing of the EUIs remained an imperative element in the preparation of the 2023 draft budget.

EDPS tried to comply with the constraints set by the current multiannual financial framework (MFF) for the period 2021-2027, which was built on the assumption that the Institutions' staffing levels remain stable and that annual inflation would not go beyond 2%.

With regard to the initial draft of the EDPS statement of estimates for 2023, a 20.1% increase of expenditure was proposed. Moreover, EDPS requested 12 additional establishment plan posts.

However, due to the extremely difficult situation for Heading 7 (European Public Administration) in 2023, the EC rejected the EDPS first proposal. In practical terms, it required additional in-depth analysis of the requested needs and several changes in the draft proposal.

Moreover, additional changes had to be applied to the salary update parameters for draft budget 2023 and all salary related budget lines had to be updated to take into account the following revised estimates:

- Salary update of 8.6% as of 1 July 2022 (12 months impact in 2023)
- Salary update of 2.6% as of 1 July 2023 (6 months impact in 2023)

In the second draft of the EDPS statement of estimates for 2023 it was proposed an overall budget increase of 10.88%, and nine additional establishment plan posts. Despite the efforts produced by the EDPS in the second proposal, further cuts were performed by the EC when consolidating the EU draft budget 2024 and the Council during the negotiation of the budget proposal with the EP.

The final outcome imposed a reduction of four establishment plan posts compared to the second proposal, and a direct decrease of EDPS capacities to recruit.

The final approved budget foresees an increase of expenditure of 9.53% compared to 2022, which implied a major reduction of the original proposal and will definitely require careful monitoring in the implementation and ad-hoc adjustment if required.

3.3.5. Discharge 2020 Budget

In October 2022, the EDPS was granted discharge³⁷ by the EP. The European Court of Auditors (ECA) did not identify any specific issues concerning the EDPS³⁸. The Budgetary Authority only formulated some minor observations in its recommendation³⁹ which the EDPS already addresses.

3.3.6 Staff

In 2022 the tendency to grow in terms of staff numbers continued. Eleven new positions (FTEs) were granted by the Budgetary Authority in 2022 to cover the responsibilities

³⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:258:FULL&from=EN>

³⁸ https://www.eca.europa.eu/Lists/ECADocuments/annualreports-2020/annualreports-2020_EN.pdf

³⁹ https://www.europarl.europa.eu/doceo/document/TA-9-2022-0152_EN.html

stemming from Regulation 2018/1725, new supervisory tasks and new tasks for the EDPB, reaching a total of 125 staff members at the end of December.

3.4 Procurement and contracting

3.4.1 Professionalization

High standards of professionalism, ethical conduct, social and environmental standards are core values of EDPS's procurement management.

The EDPS ensured equal treatment, transparency and non-discrimination and guaranteed possibilities for small and medium enterprises to have access to the market contributing for the accomplishment of social objectives such as employment and economic stability.

The EDPS constantly searches for economic operators that are capable of ensuring qualified standards and proficiency in the implementation of the awarded contracts.

The EDPS continue to pay particular attention to the safeguard of data protection rules as well as EU standards on intellectual property rights. This has required ad-hoc drafting by adapting tender documents, ensuring the fulfilment of data protection requirements related to framework contracts implementation and inserting data protection sheets as annexes to specific contracts.

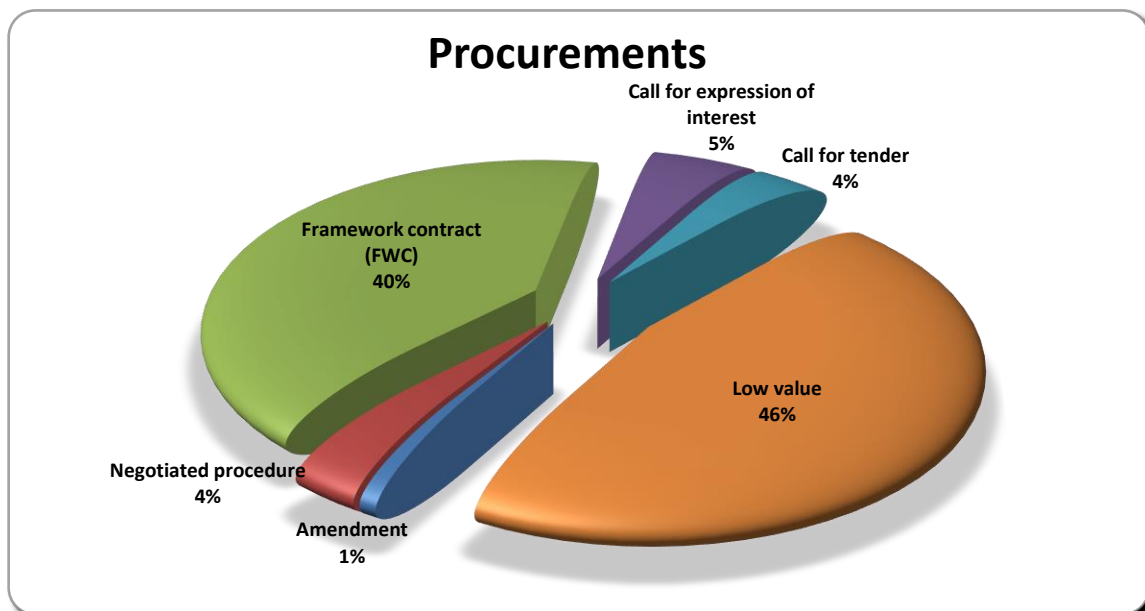
3.4.2 Framework contracts and concluded contracts

As in the previous years, in 2022 EDPS continued to participate in large inter-institutional framework contracts for increasing administrative efficiency. The most important inter-institutional framework contracts relate to IT consultancy, interim services, office supplies and office furniture.

In addition to the participation in inter-institutional procedures, the EDPS conducted one procedure itself leading to a framework contract in the communication field. From 114 procedures carried out, most of them were very low value procedures and procedures implementing existing framework contracts.

Among those, four procedures were conducted for signing direct service contracts and in all four of them, negotiated procedures without publication were used (to be reported in line with art. 74, 10 FR).

It should also be pointed out that in 2022 the EDPS launched, and is currently managing (acting for the EDPB), a call for expressions of interest aiming to establish a list of individual experts. Five specific contracts have been awarded.



3.5. Finance

Since 2020, the EDPS uses a paperless financial workflow, *Speedwell*. It can be seen as an extension of ABAC, allowing the electronic circulation of invoices between all actors involved in a payment process and guides them through the verification. The system has an ECAS⁴⁰ access which guarantees the identity of the person giving a visa, including the 'certified correct' visa of the invoice and 'passed for payment'. The implementation of this electronic workflow ensured the business continuity allowing full adaptation to the new working methods of enhanced teleworking and improved both the efficiency of the processing of financial transactions and the quality of the financial and accounting information.

Statistics related to ex-ante controls

In 2022, the number of financial transactions increased substantially compared to 2020 and 2021. This was a consequence of the 'return to normal' after the pandemic period. However, the number of transactions is still below the 2019 figures, as some activities were impacted by the new way of working (e.g. organisation of virtual or hybrid experts' meetings or participation to virtual events).

Payment requests

	2019	2020	2021	2022
Experts reimbursements	1522	319	21	281
Missions	298	69	63	216
Other	492	331	288	302
Total	2312	719	372	799

⁴⁰ EU Login authentication service

In terms of payment execution, based on the average payment amount per transaction (from EUR 6 704 in 2019 to EUR 23 766 in 2022), there is a significant growth, compared to 2019 (+23%).

Payment requests amount (in 1,000€)

	2019	2020	2021	2022	% increase since 2019
Experts reimbursements	697	144	13	128	-82%
Missions	131	34	35	210	60%
Other	14,671	14,505	16,570	18,651	27%
Total	15,499	14,683	16,618	18,989	23%

	2019	2022	
average amount by transaction (in €)	6,704	23,766	255%

As required by Art. 74.5 of the Financial Regulation, all operations are subject to ex-ante controls. These controls comprise the initiation and ex-ante verification of an operation and concern both the operational and financial aspects. They are operated by staff with the required skills appointed by the AOD.

The EDPS uses checklists listing the basic controls to be carried out by the operational and financial agents involved in the processing of the operations. The use of *Speedwell* facilitates substantially the aforementioned basic controls applied on payments and commitments.

Missions, expert payments and salaries are initiated by the Paymaster Office of the European Commission (PMO) in application of the Service Level Agreement concluded between the respective Institutions. These payments are subject to an additional layer of ex-ante controls which are operated by the PMO staff in addition to the controls applied at the EDPS.

	Total	Refused	
Commitments	161	28	17.39%
Payment Orders	587	15	2.56%
Transactions total	748	43	5.75%

(*) A payment order can contain several payment requests

3.6 Missions management

The management of missions at the EDPS is conducted in accordance with the applicable rules of the Commission's *Guide* to missions. In addition, the EDPS has a speaking engagement policy, which clarifies the rules in those cases where the mission expenses should be paid by the organiser and is selective as regards attendance to external events.

As regards mission statistics for 2022, they relate the period from January to December. As requested by the Budget Control Committee of the EP, a comparative table of the last four years is included below.

	2019		2020		2021		2022	
	Supervisor	Staff	Supervisor	Staff	Supervisor	Staff	Supervisor	Staff
Number of missions	29	301	4	39	6	57	21	171
Average cost in €	885	701	537	578	446	505	1.488	1.035
Total cost in €	17.800	207.497	2.147	22.547	2.675	28.789	31.267	176.903

As regards the Supervisor, missions are conducted with full transparency as provided in his *Code of conduct*. Further details of the missions performed by the European Data Protection Supervisor during the year can be found in Annex 4.

EDPS SUPERVISOR 2022		
NAME	N° MISSIONS	TOTAL COSTS (EUR)
Wojciech WIEWIOROWSKI	20	24 888.28

The EDPB Chair performed eight missions in 2022.

EDPB CHAIR 2022		
NAME	N° MISSIONS	TOTAL COSTS (EUR)
Andrea JELINEK	8	11 035.05

In November 2022, the EDPS joined a PMO pilot project for the management of missions in shared mode. Since then, EDPS staff going on mission can directly benefit from services offered by PMO's mission experts, notably when it comes to declarations of mission expenses and related reimbursements. The PMO mission officer is present in the visa chain for the declaration of expenses to verify that the requests for reimbursement are in accordance with mission and financial rules. For first line mission support and for the validation of mission requests, the EDPS maintains an in-house helpdesk in the HRBA unit.

4. Management and internal control

4.1 Characteristics and nature of activities

4.1.1 The mission of the EDPS

Data protection is a fundamental right, protected by European law and enshrined in Article 8 of the Charter of Fundamental Rights of the EU.

For protecting and guaranteeing the rights to data protection and privacy, the processing of personal data is subject to control by an independent authority. The EDPS is the EU's independent data protection authority, tasked with ensuring that the EUIs embrace a strong data protection culture.

In accordance with Regulation (EU) 2018/1725 (1) the EU as a policy making, legislating and judicial entity looks to the EDPS as an independent supervisor and impartial advisor on policies and proposed laws which might affect the rights to privacy and data

protection. The EDPS performs these functions by establishing itself as a centre of excellence in the law, and in technology, insofar as it affects, or is affected by the processing of personal data.

The EDPS carries out its functions in close cooperation with fellow DPAs as part of the European Data Protection Board (EDPB), and aim to be as transparent as possible in its work serving the EU public interest. Under the GDPR, the EDPS is also responsible for providing the secretariat to the EDPB.

Furthermore, the EDPS is also in charge of supervising the processing of personal data relating to activities at the EU's law enforcement agency, Europol and Eurojust. The relevant legislation in this case is Regulation (EU) 2016/794, which applies to Europol and Regulation (EU) 2018/1725 and Regulation (EU) 2018/1727, which applies to Eurojust. A similar, specific data protection regime is in place for the EPPO.

The EDPS:

- monitors and ensures the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals.
- advises EU institutions and bodies on all matters relating to the processing of personal information. EDPS is consulted by the EU legislator on proposals for legislation and new policy development that may affect privacy.
- monitors new technology that may affect the protection of personal information.
- intervenes before the EU Court of Justice to provide expert advice on interpreting data protection law.
- cooperates with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal information, in particular both as a provided of the Secretariat and member of the European Data Protection Board.

In addition, the EDPS:

- Aims to develop a culture of accountability whereby the institutions recognise their own responsibility to ensure the protection of personal data when developing new EU policies and legislation;
- Provides support to the EUIs to be accountable: to help the legislators carry out their own assessment of proposed measures implying the processing of personal data, the EDPS has developed a toolkit on the concept of necessity;
- Aims to provide pragmatic advice by analysing the complexity of a proposal and take advantage of the experience gained in its supervision cases with the EU institutions; the EPDS looks for constructive and workable solutions;
- As an advisor on all data protection matters at EU level, in addition to providing advice on a consultation by the Commission (or other institution), the EDPS also issues advice on its own initiative, when there is a matter of particular significance.
- The EDPS is not for or against any measure involving the processing of personal data and bases its assessment and advice on the evidence justifying its need.

4.1.2 Core values and guiding principles

4.1.2.1 The core values

The EDPS approach to its tasks and the way in which it works with its stakeholders are guided by the following values and principles:

- **Impartiality** – working within the legislative and policy framework given to the EPDS, being independent and objective, finding the right balance between the interests at stake.
- **Integrity** – upholding the highest standards of behaviour and to always do what is right
- **Transparency** – explaining what the organisation is doing and why, in clear language that is accessible to all.
- **Pragmatism** – understanding its stakeholders’ needs and seeking solutions that work in a practical way.

4.1.2.2 General principles

1. The EDPS serves the public interest to ensure that EU institutions comply with data protection policy and practice. He contributes to wider policy as far as it affects European data protection.
2. Using his expertise, authority and formal powers to build awareness of data protection as a fundamental right and as a vital part of good public policy and administration for EU institutions.
3. He focuses his attention and efforts on areas of policy or administration that present the highest risk of non-compliance or impact on privacy. He acts selectively and proportionately.

4.1.3 Data Protection and the EDPS in 2022

The characteristics and nature of activities at the EDPS dealing with data protection are dealt in point 2 of the present report. This sections deals only with communication and internal IT.

4.1.3.1 Communicating data protection

The reach and influence of the EDPS' communication are constantly expanding. Effective communication is vital in ensuring that information on EDPS activities reaches the relevant external audience.

With public interest in and engagement with data protection increasing, the EDPS' communication efforts in 2022 built on the successes of previous years and reinforce the status of the organisation as a respected, international leader in the data protection field. This involved sustained efforts in several areas, including online media, events, publications and external relations with press and stakeholders.

Noteworthy, considerable work was put into the preparation and promotion of the EDPS' international conference, titled “The future of data protection: effective enforcement in the digital world”, which hosted more than 2000 participants, both in-person and remotely.

The EDPS continued to inform its various stakeholders through the publication of longer forms of content on the EDPS website, such as press releases on leading EDPS Opinions on legislative proposals, monthly updates through the EDPS newsletter, the EDPS blogpost used as a platform for the Supervisor and the Head of the EDPS Secretariat to share their personal insights on data protection and its related matters. These different streams of communication allows the EDPS to reach out to diverse audience composed of both experts and non-experts in data protection.

As social media has become an indispensable communication tool for the EDPS, efforts continued to implement an effective social media strategy that helped expand its influence and reach online. With our social media channels, we continued to inform our stakeholders in a timely way on EDPS data protection activities, as well as continuing our efforts to increase the EDPS's visibility as an employer and attract new talents. To this end, the EDPS launched a few campaigns organised with its Staff Ambassadors and trainees, which gained a lot of attention on social media. In this sense, through its accounts on Twitter, LinkedIn and YouTube, the EDPS is now able to reach an increasingly diverse and global audience. What is more, the EDPS launched two other alternative social media platforms, EU Voice and EU Video, this year, as a way to reach additional stakeholders, and to ensure inclusivity in the way the EDPS shares its information. The platforms are directly accessible from the EDPS homepage.

The EDPS will continue to diversify and expand its communication activities in the coming months and years, to bring its work closer to the public, in alignment with one of the organisation core values, transparency.

4.1.3.2 EDPS IT infrastructure

Most of the IT services used by the EDPS' are supplied by the EP (e.g. network, hardware, office software, mail servers, and mobile devices). The EDPS uses also software provided by other EUIs, whereas its content management system is outsourced to a private company.

In order to steer the digital transformation propelled by the COVID-19 pandemic, the EDPS is currently reflecting on its choices on its IT infrastructure and the agility and independence of the EDPS with respect to IT. The objective would be to achieve more EDPS autonomy and control in relation to IT infrastructure with possibly creating a specific organisational team in the EDPS specifically tasked with deploying, supporting and developing the IT infrastructure (as in the EDPB).

In 2022 the EDPS procured an IT feasibility study that will be carried out in 2023. This study will be the second phase of the overall effort towards an EDPS digital transformation, whose first phase was the "IT gap analysis" carried out in 2021, which assessed the EDPS IT business requirements, inventoried IT assets and started looking at first possible solutions to fill gaps to support EDPS tasks. The results of the feasibility study will be submitted to the EDPS management as an input for a possible transformation of the EDPS IT infrastructure and tools.

4.2 Strategy 2020-2024

4.2.1 EDPS strategic objectives

The EDPS issued in June 2020 its 2020-2024 Strategy “Shaping a Safer Digital Future: a new Strategy for a new decade”. In a connected world, where data flows across borders, solidarity within Europe, and internationally, will help to strengthen the right to data protection and make data work for people across the EU and beyond. The Strategy focuses on three pillars: foresight, action and solidarity to address digital challenges for a safer, fairer and more sustainable future. Its three strategic pillars and related actions are detailed in Annex 5.

4.2.2 Action plan

The related action plan is detailed in Annex 6. This action plan is implemented and monitored through the yearly annual management plan (AMP).

4.2.3 Measuring performance

The EDPS uses a number of key performance indicators (KPIs) to help it monitor its performance in the context of the main objectives set in the EDPS Strategy. This ensures that it is able to adjust its activities, if required, to increase the impact of its work and the efficiency of its use of resources⁴¹.

The KPI scoreboard below contains a brief description of each KPI and the results on 31 December 2022. These results are measured against initial targets, or against the results of the previous year set as benchmark.

In 2022, KPIs were met or surpassed - in some cases significantly - the targets set in eight out of nine KPIs, with one (KPI8 - Occupancy rate of the establishment plan) just falling short of the set target. These results clearly illustrate the positive outcome the EDPS had in implementing the strategic objectives throughout the year, notwithstanding the challenging circumstances in which the EDPS still had to operate in the context of the Covid-19 Pandemic.

KEY PERFORMANCE INDICATORS		Results 31.12.2022	Target 2022
KPI 1 Internal indicator	Number of initiatives, incl. publications, on technology monitoring and on promoting technologies to enhance privacy and data protection organised or co-organised by EDPS	13 initiatives	10 initiatives
KPI 2 Internal & External Indicator	Number of activities focused on cross-disciplinary policy solutions (internal & external)	8 activities	8 activities

⁴¹ The KPIs were partly revised at the end of 2020, to ensure that the performance metrics adapt to developments in EDPS activities.

KPI 3 Internal Indicator	Number of cases dealt with in the context of international cooperation (GPA, CoE, OECD, GPEN, Spring Conference, international organisations) for which EDPS has provided a substantial written contribution	27 cases	5 cases
KPI 4 External Indicator	Number of files for which the EDPS acted as a lead rapporteur, rapporteur, or a member of the drafting team in the context of the EDPB	21 cases	5 cases
KPI 5 External Indicator	Number of Article 42 opinions and joint EDPS-EDPB opinions issued in response to EC legislative consultation requests	4 Joint Opinions 27 Opinions	Previous year as benchmark (17)
KPI 6 External Indicator	Number of audits/visits carried out physically or remotely	4 audits 2 visits	3 different audits/visits
KPI 7 External Indicator	Number of followers on the EDPS social media accounts ⁴²	YT- 2.75k L - 63k T - 29.1k EU Voice - 5.1k EU Video - 0.69k	Results of previous year ⁴³ + 10%
KPI 8 Internal Indicator	Occupancy rate of establishment plan	86.9%	90%
KPI 9 Internal Indicator	Budget implementation	98.2%	85%

4.3 Inter-institutional cooperation

In 2022, inter-institutional cooperation continued in the areas in which the EDPS is assisted by other EUIs.

The Commission's assistance is valuable to the EDPS in particular with regard to financial, accounting and budgetary matters. Directorate General Budget provides technical assistance to the EDPS in financial and accounting matters and the Central Financial Service assists EDPS/EDPB providing information upon request. The Commission's Accounting Officer acts simultaneously as Accounting Officer to the EDPS. The same applies to the Commission's Internal Audit Service being in charge of the internal audit activity in the organisation.

⁴² Twitter, LinkedIn, YouTube.

⁴³ YT:2.44k, L: 49.57k, T: 25.83k

Inter-institutional cooperation presents many advantages from the perspective of good financial management and budget consolidation. This cooperation is vital for the EDPS, not only because of the small size of the organisation, but also because it increases efficiency and allows for economies of scale. In addition, most of the expenditure remains within the EU administrations, therefore resulting in appreciable savings for the EU budget.

4.4 Ex-post controls

According to Art. 74.6 of the Financial Regulation, the Authorising Officer can organise, in addition to the mandatory ex-ante controls, also ex-post controls on sample basis depending on risks related to the transactions. Following an ECA observation and due to the fact that the organisation grew over the years with an increasing budget and number of financial transactions, the acting Head of EDPS Secretariat, being the Institution's AOD, decided to carry out again these controls, for 2022. To this end, a work instruction was drafted for governing the ex-post controls exercise and the controls were carried out for a sample of 12 transactions corresponding to a monetary value of EUR 2 155 358.12 (11.35% of the total 2022 EDPS/EDPB expenditure).

The ex-post controls for 2022 were completed on 10 March 2023. The results demonstrated that the legality and regularity provisions, procurement procedures as well as financial and accounting provisions are respected in the organisation and no irregularities were detected.

In two cases a late interest fee was generated. However, suspension (Art.116§4 of the Financial Regulation) could not apply as all information was available and correct. The late interest fees - being less than EUR 200 - were not claimed by the creditors (Art.116§5 of the Financial Regulation). Consequently, no quantifiable error can be determined and therefore all sampled transactions of the EDPS/EDPB are free from any material error.

4.5 Events during the year that affected reputation

There were no events during 2022 that might have had a negative impact on the institution's reputation. The teleworking scheme was smooth and did not lead to any incidents.

4.6 Internal control management system

Internal control standards (ICS) cover policies and procedures put in place by the institution to ensure the economic, efficient and effective achievement of its objectives. The latest revision of the ICS decision was done on 6 October 2020 with the formalisation of the EDPS relying on the Internal Audit Service (IAS) of the EC for ensuring the internal audit activity in the organisation.

The EDPS also establishes an annual management plan on a yearly basis. This plan shall translate the long term strategy of the EDPS into general and specific objectives. The plan sets out the activities to be undertaken by specific objectives. The annual management plan also includes the KPIs, defined in the Strategy 2020-2024, which are regularly measured, and revised if necessary, to monitor progress achieved during the implementation phase.

Since the adoption of the decision on risk management in July 2012, the EDPS perceives risk management as an essential element of its global strategy. Risk management goes beyond assessing the risks; it also involves putting controls and measures in place that need to be monitored afterwards. This assessment of risks, controls and measures in place is detailed in a risk register which is adopted, with close involvement of all managers of the organisation every year.

The 2022 risk register was formally adopted on the 22 April 2022 following its presentation at the Management Meeting on 30 March 2022. The 2022 concluded in formulating 17 risks out of which none was ranked 'critical'. Most of the risks identified, have as root cause the lack of human resources. Due to the increase of work of the EDPS and the EDPB, these risks will likely remain in the near future. For the four with the highest score, a follow-up was carried out in October 2022, which confirmed their likelihood and impact as identified initially.

In 2022, the EDPS elaborated a revised framework for the risk management in the organisation. This revised framework was used as pilot at the end of 2022 for carrying out the 2023 risk assessment exercise. Novelties of the revised framework include the Head of the EDPS Secretariat launching the exercise instead of the ICC for setting the 'tone at the top', linking the exercise with the preparation of the annual management plan for embedding risk-thinking in the planning of activities phase, meeting between senior and middle managers for discussing and concluding on the identified risks, introducing a structured follow-up for those risks defined by management as very important to be followed up and establishing a risk inventory serving as a database for tracking and monitoring all risks from recent exercises. The 2023 exercise was completed on 27 February 2023, identifying 24 risks (19 for the EDPS and the 5 for the EDPB) out of which none was ranked 'critical'. The new framework will be formally adopted in Q2 2023 after integrating the lessons learnt and best practices.

These controls put in place by the EDPS, along with the procedural channels, are intended to correct any financial or procedural error that might arise. They are an integral part of the management of the EDPS, as are any corrections to which they give rise. The AOD is thus aware of any corrections. Neither the nature nor the frequency of the identified risks has been significantly relevant.

4.7 Internal evaluation of the internal control system and indicators underpinning the statement of assurance

The monitoring of the implementation of the ICS is the responsibility of the ICC, who reports directly to the Head of EDPS Secretariat.

During 2022, the EDPS marked a considerable improvement of the internal control systems. Some indicative examples refer to the solid ethics process in place, the update of processes and procedures concerning HR management being modernised even more in the post-covid era, the improvement of its IT governance, the establishment of the Head of the EDPS Secretariat position optimising the chain of command in the organisation, the relaunch of the ex-post controls and the update of the risk management framework.

Beyond certain areas of improvement (see section 4.9.3) the internal control systems of the EDPS is compliant and carries out the appropriate monitoring activities for improving its efficiency. The action plan following the staff satisfaction survey of 2022, will only add to the efficiency of the organisation, once available.

At this stage, the AOD estimates that the level of management and control put in place is appropriate and improving. Such improvements are not likely to have a 'material' impact within the meaning of paragraph 0. No reservations are necessary with regard to the improvements underway.

At the time of writing this annual activity report, no significant errors have occurred, and no reservations are necessary as regards preventive controls.

4.8 Cost effectiveness and efficiency of Internal Control

Being a small Institution, the EDPS has neither the means nor the resources to carry out a classic cost-benefit analysis. Therefore, the organisation takes as a base the model applied by EPSO, since this office, as the EDPS, only manages administrative appropriations under Heading V of the EU budget. This model consists of a single global indicator which is calculated by dividing the approximate total cost of control by all expenditure made during the year (budget implementation in terms of payments).

The total number of FTEs involved in the main control activities (internal control, procurement and finance) is estimated at around 6 FTEs.

The estimated average cost (all categories of cost included) of the control activities for 2022 would be EUR 714 121.

The total budget implementation in terms of payments for 2022 is EUR 18 988 909.76. It means that the cost of the control activities represents 3.76% of the EDPS expenditure.

4.9 Results of independent audit during the year

There are two independent auditors for the EDPS: the European Court of Auditors (ECA) and the EC IAS who acts as the EDPS Internal Auditor.

4.9.1 Court of Auditors

In 2022, the ECA work in the EDPS was the following:

- I. completed the 'Statement of Assurance' 2021 and carried out a follow-up of previous years' observations,
- II. issued its Annual Report for 2021 and
- III. carried out the Statement of Assurance for 2022.

4.9.1.1 Statement of Assurance (SoA) 2021 and follow-up of previous years' observations

Within the framework of the SoA 2021, the ECA examined one financial transaction, items from the exceptions and non-compliance register and the provisional and final accounts. No error was detected concerning the EDPS.

The analysis of the AAR 2021 by the ECA, revealed some discrepancies concerning the ECA work in the EDPS, which were diligently corrected in the current AAR.

As far as it concerns the follow-up of previous years' observations, the ECA maintained the two following observations open:

1. Establishment of an Audit Progress Committee (APC) (FRArt.123)
2. Weaknesses in the ex-post verification process and inadequate disclosure of results in the annual declaration of assurance

Concerning the open observations, the EDPS acknowledged the benefits of setting up an APC, however the Internal Control Coordinator (ICC) - as from 2022 one FTE - ensures an effective monitoring of recommendations' implementation, maintaining the number of EDPS very important overdue⁴⁴ recommendations from the IAS, to zero. This category of recommendations is in principle, but not exclusively, under scrutiny from an APC.

Concerning the ex-post controls, these were carried out for the financial year 2022 (see section 4.4). The lessons learnt from this exercise will serve to further improve and crystallise the process.

4.9.1.2 The ECA Annual Report 2021

On 13 October 2022 the ECA published its Annual Report for 2021⁴⁵. The EDPS is quoted under Chapter nine 'European public administration'. Within the sample of 60 transactions - including other institutions as well (one for EDPS) - the ECA made no reference to the EDPS as it did not identify and specific issues.

4.9.1.3 Statement of Assurance 2022

Within the 2022 Statement of Assurance exercise, the ECA sampled one EDPS transaction which did not give rise to any observations. The full results of the SoA 2022 are still to be finalised.

The ECA took note that the EDPS performed an ex-post control exercise for the financial year 2022. Nevertheless, it considers that there is space for improvement of the process and will continue to examine the ex-post reports and the disclosure of the results in the Annual Activity Reports on the annual basis.

4.9.2 Internal Audit Service (IAS)

During 2022, the IAS completed the follow-up audit of all recommendations stemming from the audit on the supervision of the processing of personal data by Europol by the EDPS. It concluded that all recommendations have been adequately and effectively implemented except one action under one recommendation. Due to the progress made towards implementing this recommendation, it was downgraded from 'very important' to 'important'. Consequently, three 'very important' and two 'important' recommendations were 'closed' by the IAS.

The pending action referred to updating the system owner term for ensuring alignment with the security rules for protecting EU Classified information (EUCI). Indeed, the EDPS implemented this action in November 2022 through the update of the relevant decision. The progress and the supporting documents were submitted to the IAS immediately after. On 27 February 2023, the follow-up for this pending action was initiated. Till submission of the present annual activity report, the outcome of this follow-up has not been completed.

The current state of play was confirmed by the IAS in its 2022 Annual Report for the EDPS, issued on 21 February 2023.

⁴⁵ <https://www.eca.europa.eu/en/Pages/AR2021.aspx>

Recommendation / Issue type	Risk rating	Status
Follow-up of EDPS recommendations by Europol	Very important	Closed
Controls for handling EUCI within the context of supervisory activities	Very important	Closed
Service provider management	Very important	Closed
IT Security Governance	Downgraded from very important to important due to progress made	One action pending IAS review
Establishing the supervisory strategy	Important	Closed
Technical guidelines for performing supervisory activities	Important	Closed

In addition, the IAS carried out the annual risk assessment exercise for updating its 2023 audit plan for the EDPS. As a reminder, the three-year risk assessment for establishing the 2022-2024 Strategic Internal Audit Plan (SIAP) for the EDPS was conducted during the Q3 and Q4 of 2021. Under the SIAP 2022-2024 two audit topics had been identified: a) the risk assessment methodology for the planning of the EDPS audits and b) governance arrangements for IT services provided by the European Parliament to the EDPS.

The 2023 audit plan for the EDPS confirmed the audit topic under point a) above. The audit was announced on 12 December 2022. The opening meeting took place on the 19 January 2023 and the audit is currently at the preliminary survey⁴⁶ stage. The final audit report is expected in Q4 2023.

4.9.3 Internal Control Standards (ICS) monitoring situation

Based on the EDPS decision of 06 October 2020 on the adoption of the ICS, their assessment is done through examination of 14 standards, grouped up in six building blocks:

- I. Mission and values
- II. Human Resources
- III. Planning and Risk Management Processes
- IV. Operations and Control Activities
- V. Information and Financial Reporting

⁴⁶ Collection of input, understanding of the process for defining the audit scope.

VI. Evaluation and Audit

The 2022 ICS assessment report was issued on 30 March 2023. The assessment concluded that the overall level of internal control is satisfactory. All six building blocks are present and functioning. The effectiveness of building blocks II and IV above could be improved. More precisely, the effectiveness of ICS 3, 4, 7, 8, 10 and 11⁴⁷ could be enhanced by improving the monitoring of the staff turnover and the establishment of preventive measures, the perception of the staff on learning and development activities, the IT governance structure, the exceptions assessment and close monitoring, the update of the business continuity plan and the finalisation of a structured process for knowledge management.

Following the results of the 2022 staff satisfaction survey, an action plan is anticipated. Ultimately, this action plan together with a close monitoring of the areas where there is space for improvement, will enhance the effectiveness of the internal control in the organisation.

4.9.4 Discharge procedure

On 4 May 2022, the EP granted the EDPS discharge with respect to the implementation of the budget for the financial year 2020⁴⁸.

For the year 2021, the EDPS responded in October 2022 to 53 questions of the EP concerning budgetary and financial management, the ethical framework and transparency, digitalisation, cybersecurity and data protection, buildings, environment and sustainability, interinstitutional cooperation and communication. The outcome on the discharge procedure for 2021, is expected for Q2 2023.

4.10 Conclusions on the effectiveness of internal control

In light of the information above, the authorising officer by delegation considers that the overall internal control system is compliant and certain improvements can be made, bearing in mind the level of expenditure and budget handled by the institution, and thus gives the necessary assurance to his annual statement.

5. Reservations and impact on the statement

5.1 Materiality criteria

In order to establish the Statement of Assurance the AOD applies the materiality criteria adopted by the Court of Auditors.

⁴⁷ ICS3: Staff allocation and mobility, ICS4: Staff evaluation and development, ICS7: Operational Structure, ICS8: Processes and procedures, ICS10: Business continuity and ICS11: Document management

⁴⁸ https://www.europarl.europa.eu/doceo/document/TA-9-2022-0152_EN.html#title1

5.1.1. Objectives of materiality criteria

The materiality threshold gives the AOD a basis on which to establish the significant weaknesses that require a formal⁴⁹ reservation to his statement. The assessment of a weakness falls to the qualitative and quantitative judgment of the AOD, who remains responsible for the statement of assurance, including the reservations made.

The purpose of this chapter is to define the qualitative and quantitative criteria for determining the level of materiality.

5.1.2. Qualitative criteria

The following parameters were used to establish significant weaknesses:

- significant/repeated errors without mitigation;
- weakness in the internal control system;
- insufficient supporting documents;
- material problems identified by the ECA or the IAS;
- problems of reputation;

5.1.3. Quantitative criteria

Once a significant weakness has been identified, quantitative criteria must be applied to determine the level of materiality. This level will be used to determine whether the weakness 'merits' being reported.

- margin of error
- maximum amount of risk.

The ECA uses a 2% materiality threshold. Should the residual risk of an error be higher, the institution must explain the reasons for it.

The EDPS has decided on 2% of annual appropriations as the materiality threshold in this regard, namely: EUR 405 320 (2% of the 2022 budget after transfers)

5.1.4. Criteria of the Internal Audit Service

A 'table of significance' is added to the internal auditors' report. In this table, a distinction is made between recommendations and observations on the one hand, and levels of importance on the other: critical, very important, important and desirable. According to the internal auditors, only 'critical' level observations *may* result in a reservation in the statement given in the annual activity report. For the EDPS, there are no observations at this level, as indicate in Section 4.9.2 above.

5.2 Reservations

No reservation.

5.3 Conclusion

Based on the above, the acting Head of the EDPS Secretariat has issued the annual statement with no reservation.

⁴⁹ The Commission (COM (2003)28 of 21 January 2003) considers that only 'material' reservations can be used to qualify the annual statement.

6. Statement of assurance from the authorising officer by delegation

I, the undersigned, Leonardo CERVERA NAVAS, acting Head of the EDPS Secretariat, in my capacity as authorising officer by delegation

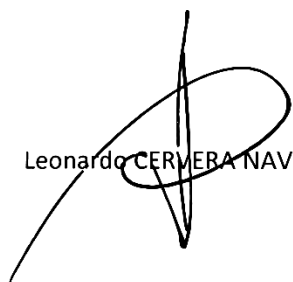
Declare that the information contained in this report gives a true and fair view.

State that I have had reasonable assurance that the resources allocated to the activities described in this report have been used for the intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying operations.

This reasonable assurance is based on my own judgment and on the information available to me, such as the results of the self-evaluation, ex-post controls and the report of the Internal Audit Service.

Confirm that I am not aware of any matter not reported here which could harm the interests of the institution.

Brussels, 31 March 2023


Leonardo CERVERA NAVAS

Head of EDPS Secretariat (acting)

7. Annexes

Annex 1: Summary of annual activity report

The Financial Regulation (Article 74.9)⁵⁰ provides that the annual activity report for the financial year of the authorising officer of Union institutions, Union bodies, European offices and agencies shall be published by 1 July of the following financial year on the website of the respective Union institution.

Following the report on discharge in respect of the implementation of the general budget of the European Union for the financial year 2016 issued on 26 March 2018, the European Parliament requested to set a deadline for the submission of the annual activity reports of 31 March of the year following the accounting year.

Alongside this, Article 60 of Regulation (EC) No 2018/1725 provides that the EDPS shall submit an annual report on his/her activities to the European Parliament, the Council and the Commission. The proposal is thus to summarise the authorising officer by delegation's annual activity report and include this summary in the activity report that is provided for in Article 60 of Regulation (EC) No 2018/1725:

Overall, the European Data Protection Supervisor considers that the internal control systems in place provide reasonable assurance as to the legality and regularity of the operations for which the institution is responsible.

The European Data Protection Supervisor will ensure that his authorising officer by delegation continues his efforts to guarantee that the reasonable assurance given in the statement attached to his activities report is effectively backed up by appropriate internal control systems.

⁵⁰ Financial Regulation, Article 74(9): The authorising officer by delegation shall report to his or her Union institution on the performance of his or her duties in the form of an annual activity report containing financial and management information, including the results of controls, declaring that, except as otherwise specified in any reservations related to defined areas of revenue and expenditure, he or she has reasonable assurance that:

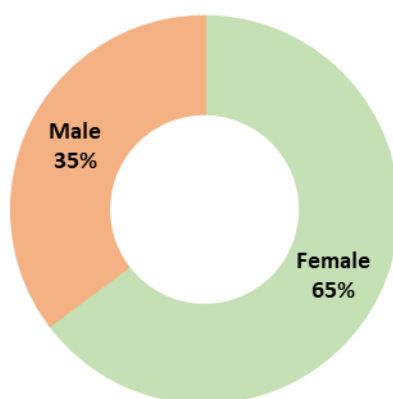
- (a) the information contained in the report presents a true and fair view;
- (b) the resources assigned to the activities described in the report have been used for their intended purpose and in accordance with the principle of sound financial management; and
- (c) the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

The annual activity report shall include information on the operations carried out, by reference to the objectives and performance considerations set in the strategic plans, the risks associated with those operations, the use made of the resources provided and the efficiency and effectiveness of internal control systems. The report shall include an overall assessment of the costs and benefits of controls and information on the extent to which the operational expenditure authorised contributes to the achievement of strategic objectives of the Union and generates EU added value. The Commission shall prepare a summary of the annual activity reports for the preceding year.

The annual activity reports for the financial year of the authorising officers and, where applicable, authorising officers by delegation of Union institutions, Union bodies, European offices and agencies shall be published by 1 July of the following financial year on the website of the respective Union institution, Union body, European office or agency in an easily accessible way, subject to duly justified confidentiality and security considerations.

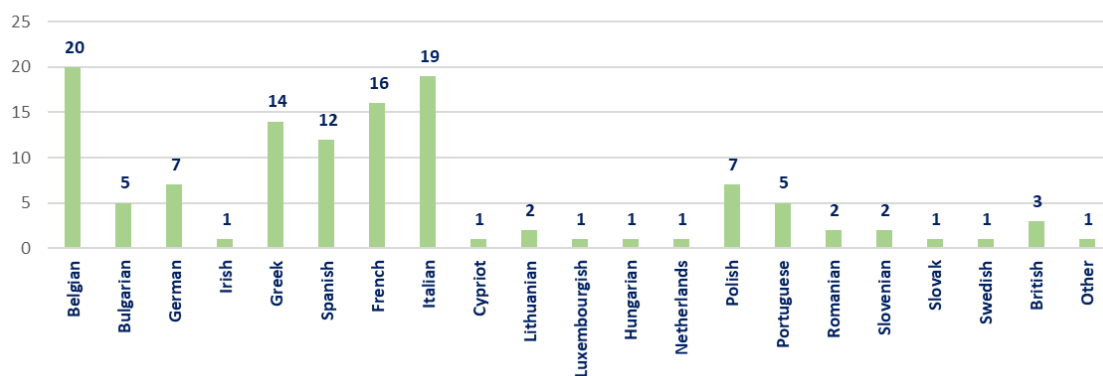
Annex 2: Human resources at the EDPS

Staff members per gender



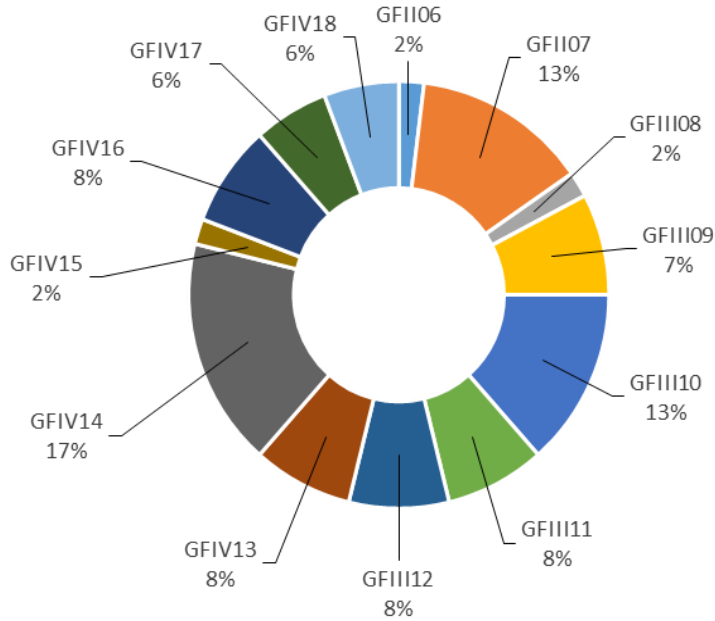
Data on 31/12/2022

Staff Members per nationality



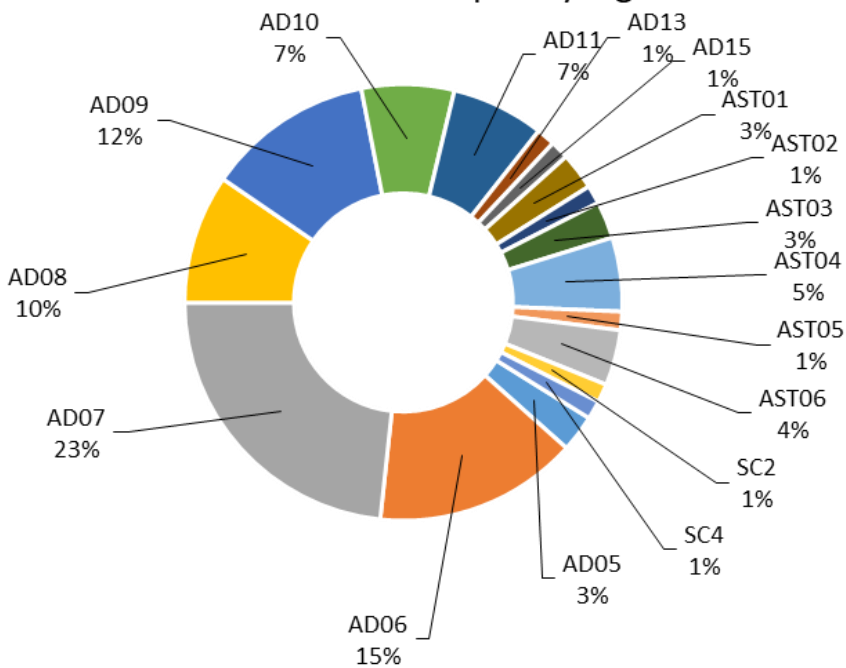
Data on 31/12/2022

Contract Agents



Data on 31/12/2022

Officials and Temporary Agents



Data on 31/12/2022

Annex 3: Budget 2022

TITLE 1 - EXPENDITURE RELATING TO PERSONS WORKING WITH THE INSTITUTION		2021 (after transfers)	Execution 2021	2022 (after transfers)	2022 vs 2021	2021 vs 2020 (%)	execution 2022 (%)
Chapter 10	Members of the institution						
Article 100	Remuneration, allowances and other entitlements of Members						
	Item 1000 Remuneration and allowances	416,168.00	96.50%	395,000.00	-21,168.00	-5.09%	97.86%
	Item 1001 Entitlements on entering and leaving the service	0.00		0.00	0.00		
	Item 1002 Temporary allowances	0.00		0.00	0.00		
	Item 1003 Pensions	0.00		0.00	0.00		
	Item 1004 Provisional appropriation	0.00		0.00	0.00		
	TOTAL Article 100	416,168.00	96.50%	395,000.00	-21,168.00	-5.09%	97.86%
Article 101	Other expenditure in connection with Members						
	Item 1010 Further training	15,000.00	8.07%	0.00	-15,000.00	-100.00%	
	Item 1011 Mission expenses, travel expenses and other ancillary expenditure	33,000.00	15.15%	33,000.00	0.00	0.00%	100.00%
	TOTAL Article 101	48,000.00	12.94%	33,000.00	-15,000.00	-31.25%	100.00%
	TOTAL Chapter 10	464,168.00	87.86%	428,000.00	-36,168.00	-7.79%	98.03%
Chapter 11	Staff of the institution						
Article 110	Remuneration, allowances and other entitlements of officials and temporary staff						
	Item 1100 Remuneration and allowances	6,405,000.00	93.46%	6,534,000.00	129,000.00	2.01%	99.98%
	Item 1101 Entitlements on entering, leaving the service and on transfer	110,000.00	94.80%	49,000.00	-61,000.00	-55.45%	98.29%
	Item 1102 Overtime	0.00		0.00	0.00		
	Item 1103 Special assistance grants	0.00		0.00	0.00		
	Item 1104 Allowances and miscellaneous contributions in connection with early termination of service	0.00		0.00	0.00		
	Item 1105 Provisional appropriation	0.00		0.00	0.00		
	TOTAL Article 110	6,515,000.00	93.48%	6,583,000.00	68,000.00	1.04%	99.96%
Article 111	Other staff						
	Item 1110 Contract staff	1,444,000.00	98.39%	2,081,228.02	637,228.02	44.13%	100.00%
	Item 1111 Cost of traineeships and staff exchanges	207,111.00	94.09%	160,971.98	-46,139.02	-22.28%	98.86%
	Item 1112 Services and work to be contracted out	54,889.00	96.95%	33,800.00	-21,089.00	-38.42%	100.00%
	TOTAL Article 111	1,706,000.00	97.82%	2,276,000.00	570,000.00	33.41%	99.92%
Article 112	Other expenditure in connection with staff						
	Item 1120 Mission expenses, travel expenses and other ancillary expenditure	72,500.00	42.66%	145,000.00	72,500.00	100.00%	100.00%
	Item 1121 Recruitment costs	6,789.00	50.41%	11,000.00	4,211.00	62.03%	100.00%
	Item 1122 Further training	83,000.00	51.55%	60,000.00	-23,000.00	-27.71%	100.00%
	Item 1123 Social service	0.00		0.00	0.00		
	Item 1124 Medical service	21,000.00	84.96%	23,000.00	2,000.00	9.52%	100.00%
	Item 1125 Union nursery centre and other day nurseries and after-school centres	83,000.00	100.00%	99,893.35	16,893.35	20.35%	100.00%
	Item 1126 Relations between staff and other welfare expenditure	88,000.00	82.69%	6,106.65	-81,893.35	-93.06%	72.93%
	TOTAL Article 112	354,289.00	70.77%	345,000.00	-9,289.00	-2.62%	99.52%
	TOTAL Chapter 11	8,575,289.00	93.40%	9,204,000.00	628,711.00	7.33%	99.94%
	TOTAL TITLE 1	9,039,457.00	93.12%	9,632,000.00	592,543.00	6.56%	99.85%

TITLE 2 - BUILDINGS, EQUIPMENT AND EXPENDITURE IN CONNECTION WITH THE OPERATION OF THE INSTITUTION		2021 (after transfers)	Execution 2021	2022 (after transfers)	2022 vs 2021	2021 vs 2020 (%)	execution 2022 (%)
Chapter 20	Buildings, equipment and expenditure in connection with the operation of the institution						
Article 200	Rents, charges and buildings expenditure	1,239,899.00	98.57%	1,610,000.00	370,101.00	29.85%	100.00%
	TOTAL Article 200	1,239,899.00	98.57%	1,610,000.00	370,101.00	29.85%	100.00%
Article 201	Expenditure in connection with the operation and activities of the institution						
	Item 2010 Information technology equipment and services	1,007,237.00	61.52%	852,000.00	-155,237.00	-15.41%	98.52%
	Item 2011 Furnitures, office supplies and telecommunication costs	38,000.00	42.19%	19,000.00	-19,000.00	-50.00%	100.00%
	Item 2012 Other operating expenditure	252,000.00	87.72%	231,000.00	-21,000.00	-8.33%	95.18%
	Item 2013 Translation and interpretation costs	509,000.00	86.03%	510,000.00	1,000.00	0.20%	100.00%
	Item 2014 Expenditure on publishing and information	102,500.00	58.36%	174,000.00	71,500.00	69.76%	95.84%
	Item 2015 Expenditure in connection with the activities of the institution	184,000.00	43.87%	366,000.00	182,000.00	98.91%	95.84%
	Item 2016 Experts reimbursements	50,000.00	3.50%	60,000.00	10,000.00	20.00%	88.63%
	TOTAL Article 201	2,142,737.00	67.06%	2,212,000.00	69,263.00	3.23%	97.60%
	TOTAL CHAPTER 20	3,382,636.00	78.61%	3,822,000.00	439,364.00	12.99%	98.61%
	TOTAL TITLE 2	3,382,636.00	78.61%	3,822,000.00	439,364.00	12.99%	98.61%

TITLE 3 - EUROPEAN DATA PROTECTION BOARD (EDPB)	2021 (after transfers)	Execution 2021	2022 (after transfers)	2022 vs 2021	2021 vs 2020 (%)	execution 2022 (%)
Article 300 Rents, charges and buildings expenditure						
Item 3000 Rents, charges and buildings expenditure	626,000.00	73.24%	633,000.00	7,000.00		100.00%
TOTAL Article 300	626,000.00	73.24%	633,000.00	7,000.00		100.00%
Article 301 Remuneration, allowances and other entitlements of officials and temporary staff						
Item 3010 Remuneration and allowances	1,446,000.00	93.91%	1,479,000.00	33,000.00	2.28%	97.60%
Item 3011 Entitlements on entering, leaving the service and on transfer	25,000.00	84.94%	26,000.00	1,000.00	4.00%	77.93%
Item 3012 Allowances and miscellaneous contributions in connection with early termination of service						
TOTAL Article 301	1,471,000.00	93.76%	1,505,000.00	34,000.00	2.31%	97.27%
Article 302 Other staff						
Item 3020 Contract staff	1,150,000.00	93.30%	1,489,000.00	339,000.00	29.48%	99.00%
Item 3021 Cost of traineeships and staff exchanges	90,000.00	83.75%	41,000.00	-49,000.00	-54.44%	74.21%
Item 3022 Services and work to be contracted out	64,000.00	83.57%	0.00	-64,000.00	-100.00%	
TOTAL Article 302	1,304,000.00	92.16%	1,530,000.00	226,000.00	17.33%	98.34%
Article 303 Other expenditure in connection with staff of the Board						
Item 3030 Mission expenses, travel expenses and other ancillary expenditure	45,000.00	4.11%	43,000.00	-2,000.00	-4.44%	100.00%
Item 3031 Recruitment costs	3,000.00	98.13%	4,929.00	1,929.00	64.30%	100.00%
Item 3032 Further training	30,000.00	49.40%	19,135.00	-10,865.00	-36.22%	100.00%
Item 3033 Medical service	4,000.00	100.00%	10,000.00	6,000.00	150.00%	100.00%
Item 3034 Union nursery centre and other day nurseries and after-school centres	32,000.00	0.00%	48,936.00	16,936.00	52.93%	100.00%
TOTAL Article 303	114,000.00	20.71%	126,000.00	12,000.00	10.53%	100.00%
Article 304 Expenditure in connection with the operation and activities of the Board						
Item 3040 EDPB plenaries and sub-group meetings	526,000.00	2.65%	145,000.00	-381,000.00	-72.43%	87.67%
Item 3041 Translation and interpretation costs	1,564,000.00	84.04%	1,107,000.00	-457,000.00	-29.22%	90.50%
Item 3042 Expenditure on publishing and information	130,000.00	44.56%	133,000.00	3,000.00	2.31%	92.83%
Item 3043 Information technology equipment and services	754,000.00	79.23%	1,106,000.00	352,000.00	46.68%	94.69%
Item 3044 Furnitures, office supplies and telecommunication costs	15,000.00	84.62%	10,000.00	-5,000.00	-33.33%	100.00%
Item 3045 External consultancy and studies	342,000.00	82.85%	252,000.00	-90,000.00	-26.32%	97.87%
Item 3046 Other expenditure in connection with the activities of the EDPB	65,000.00	3.01%	136,000.00	71,000.00	109.23%	90.66%
Item 3047 Other operating expenditure	77,000.00	66.90%	84,000.00	7,000.00		99.99%
Item 3048 EDPB Chair and Vice chairs expenses	53,100.00	12.31%	45,000.00	-8,100.00		66.66%
TOTAL Article 304	3,526,100.00	66.03%	3,018,000.00	-508,100.00	-14.41%	92.56%
TOTAL CHAPTER 30	7,041,100.00	76.57%	6,812,000.00	-229,100.00	-3.25%	95.73%
TOTAL TITLE 3	7,041,100.00	76.57%	6,812,000.00	-229,100.00	-3.25%	95.73%
TOTAL BUDGET	19,463,193.00	84.61%	20,266,000.00	802,807.00	4.12%	98.23%

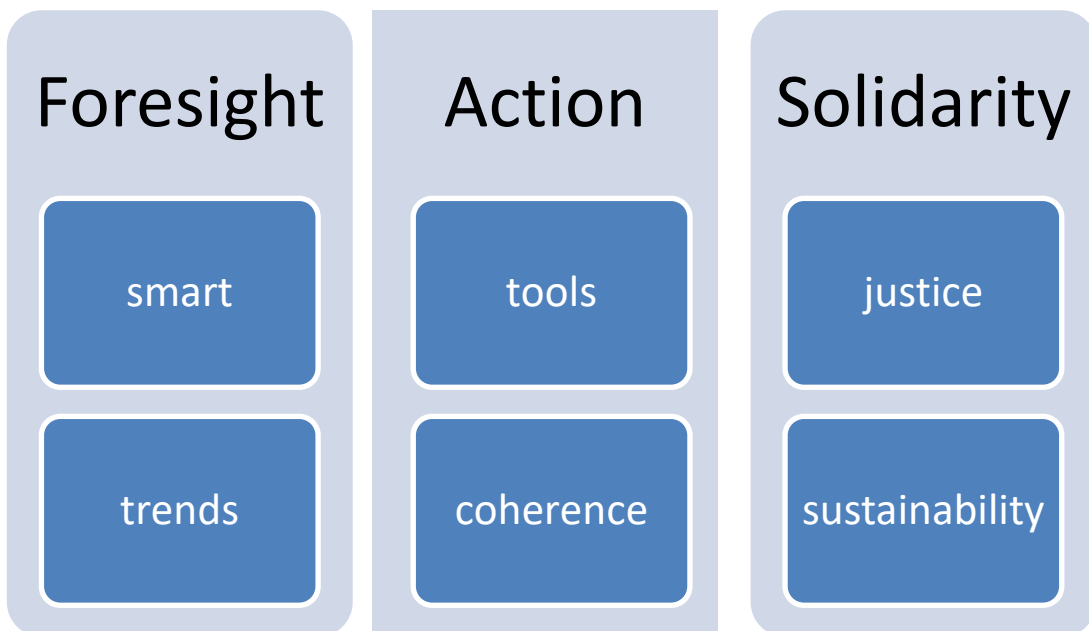
Annex 4: Detailed list of missions undertaken by the Supervisor (2022)

Wojciech WIEWIOROWSKI			
Mission Purpose	Date from	Date to	Cost
Speaker information: "Digital Investigative Measures - Towards Empirical Legal Assessment?" (1 Deember 2022)	30/11/2022 14:00	01/12/2022 17:30	68,60
ICRC Symposium	07/11/2022 15:00	08/11/2022 21:30	180,00
Meeting Europol 20 October	20/10/2022 08:30	20/10/2022 18:00	40,56
On December 7, 2022 Protection of legal secrecy in online services", Warsaw	05/12/2022 10:55	07/12/2022 23:45	1.162,23
GPA event and JPSG in Brussels	22/10/2022 11:25	24/10/2022 10:30	120,95
GPA event in Istanbul	25/10/2022 07:15	29/10/2022 21:50	1.644,45
12 October Meeting with the Head of Administration Mr Emmanuel Maurage, EIGE Vilnius 13 October EU-LISA conference Swissotel Tallinn	12/10/2022 09:20	15/10/2022 20:05	1.877,36
Digital Law & Policy Proportionality Principle In IT Regulation Warsaw	09/09/2022 17:45	11/09/2022 18:45	1.249,12
Forum for EU-US Legal-Economic Affairs WASHINGTON Cosmos Club – September 18-21, 2022	18/09/2022 12:00	24/09/2022 15:00	7.150,39
44th Global Privacy Assembly Istanbul	22/10/2022 11:25	29/10/2022 21:50	212,35
Keynote speech in Opening Programme of Advanced Master in Privacy, Cybersecurity and Data Management in Maastricht	05/09/2022 11:30	08/09/2022 22:00	939,60
PL&B Conference? Cambridge, UK	04/07/2022 15:56	06/07/2022 21:13	688,78
To give a lecture and a master lesson at Leiden University	02/06/2022 07:30	02/06/2022 20:30	185,83
IPEN Workshop on Digital Identity 22 June ENISA Invitation to the Annual Privacy Forum 2022 23_24 June	21/06/2022 19:35	24/06/2022 20:15	901,97
Meeting in Berlin, the organisers will covered the hotel expenses	15/05/2022 20:50	16/05/2022 20:10	850,15
IO workshop 12-13 May 2022 Data Protection within International organisations	11/05/2022 14:55	12/05/2022 23:25	872,11
Commissioners' meeting in Vienna, 26-28 April 2022	26/04/2022 15:40	28/04/2022 19:15	1.031,93
Spring Conference of European Data Protection Authorities 2022, Dubrovnik/Cavtat	18/05/2022 09:45	21/05/2022 05:30	1.252,55
IAPP Global Privacy Summit and DPA Day - April 11-13 in Washington Several meetings on 14 April	09/04/2022 12:00	18/04/2022 07:15	2.594,08
Privacy Symposium Conference 2022 - Venice	04/04/2022 10:15	07/04/2022 22:35	1.865,26

Annex 5: EDPS strategic objectives

The EDPS strategy describes how it intends to carry out its statutory functions and deploy the resources available to address these challenges. There are three pillars to the strategy, each reflecting its values.

- **Foresight:** the EDPS commitment to being a **smart** institution that takes the long-term view of **trends** in data protection and the legal, societal and technological context.
- **Action:** proactively develop **tools** for EUI to be world leaders in data protection. To promote **coherence** in the activities of enforcement bodies in the EU with a stronger expression of genuine European solidarity, burden sharing and common approach.
- **Solidarity:** the EDPS belief is that **justice** requires privacy to be safeguarded for everyone, in all EU policies, while **sustainability** should be the driver for data processing in the public interest.



Annex 6: EDPS strategic objectives and its Action Plan

Our objectives: what we aim to achieve by the end of 2024

The strategic objectives under the three pillars express what we intend to achieve by 2024. A number of strategic initiatives will support the achievement of those objectives. We will take more actions than can be described in this strategy; all of these will appear in our Annual Management Plan for each year of this mandate. This strategy is a live, iterative document. It will be kept under regular review as a reference point for our staff and stakeholders.

Foresight

EDPS to be a recognised and respected centre of expertise that helps understand the impact of the design, evolution, risks and deployment of digital technology on the fundamental rights to privacy and data protection.

1.1 Smart

We want to be a smart administration in a smart EUI environment

Knowledge is an essential asset for the EDPS to effectively support strategic objectives. However, we do not want to be a centre of excellence in a way that does not benefit the outside world. We want to share knowledge, expertise and contribute to the smart administration of the EUI environment.

Our aim is to use the best expertise and latest sustainable technology, to look after our people, promote diversity in all its forms, as well as being transparent and inclusive towards our stakeholders.

Hence, this part of the strategy is dedicated to outline the specific actions for this mandate.

To this extent, we will:

- Carefully monitor jurisprudence, pursue our interventions in cases before the Court of Justice of the European Union (CJEU).
- Make an inventory of the measures introduced by EUI during the Covid-19 crisis. Distinguishing those that have naturally developed from the measures that were only accelerated due to extraordinary circumstances. The latter should be recognised as temporary and discarded when the crisis is over.
- Plan a simple and short online training module for all new EUI staff and propose that this becomes compulsory. We will equip [Data Protection Officers \(DPOs\)](#) with the tools they need and help build a 'satellite' network of data protection experts.
- Organise evidence-based discussions on intrusive, emerging or hypothetical practices, such as eHealth, biometric technologies and automatic recognition systems, quantum computing, edge computing and blockchain.

- Engage with experts from the public health community in the EU and other international organisations, to better understand the needs for epidemiological surveillance and accurately measure the efficiency and purpose of the tools being developed with regard to personal data protection (e.g. by developing together practical guidance on data protection by design).
- Continue to facilitate discussions between data protection experts, regulators and the research community, including ethics boards, to ensure that data protection enhances the efforts of genuine scientific research.
- Collaborate more closely with academia and independent researchers by setting up a research visitor programme, hosting events and supporting summer academies in close cooperation with the EDPB and other DPAs. We will encourage and facilitate more exchanges between our staff and DPAs and between DPAs themselves.
- Publish case law digests concerning data protection and privacy at EU level.
- Keep exchanging information and best practices with international organisations and interlocutors in third countries.
- To study and prioritise the impacts of data processing practices on individuals and groups, especially those in vulnerable situations, such as refugees and children.
- Invest in knowledge management to ensure the highest quality of our work and to recruit a diverse, inter-disciplinary and talented workforce.

1.2 Trends

We want to know what is going on and what is going to happen

The EDPS places strategic importance on integrating the technological dimension of data protection into our work. As a data protection supervisory authority, we must closely examine both the potential risks and opportunities offered by these advances, understand the possibilities of new technologies and, at the same time, encourage the integration of data protection by design and data protection by default in the innovation process.

We aim to explain in a simple way the interaction between these trends, and to include data protection in the new EU skills agenda. In our work with the EDPB, as well as an advisor to the EUI, we focus on areas where the interests of data protection interacts with technology and other areas of law, including competition law, consumer law, finance and payment services.

The EDPS is uniquely positioned to monitor developments in the [Areas of Freedom, Security and Justice \(AFSJ\)](#). This is particularly emphasised through our role as supervisory authority of Europol, Eurojust, EPPO, Frontex, EASO⁵¹ or eu-LISA⁵².

⁵¹ EASO : European Asylum Support Office

⁵² The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

- We will actively follow the evolution of data processing practices and technology that may have an impact on privacy and data protection. We will continue to issue reports on emerging technology issues. Moreover, we will promote the understanding of what is the ‘state of the art’ of a specific technology, such as anonymisation, encryption, and network security.
- Where the European Commission proposes measures with data protection implications, we will continue to provide legal advice regarding compliance with the EU Charter and the principles of data protection set out in applicable legislation.
- We will focus on the potential impact of technology-driven policy, as recently demonstrated in our [opinions](#) on the European Commission’s “White paper on Artificial Intelligence: A European approach to excellence and trust”, and the European Commission’s Communication on “A European strategy for data”.
- Where EUI intend to deploy new technologies, we will systematically request them to clearly explain the impact of these technologies and their risks on individuals and groups.
- We will alert EUI and the public when digital technology is deployed in a way that does not respect the essence of the fundamental rights of personal data protection, privacy and other rights and freedoms enshrined in the EU Charter of Fundamental Rights.
- We strive to do this in close collaboration with the European Commission, other EUI and agencies active in related areas, such as the Fundamental Rights Agency (FRA) or the European Agency for Cybersecurity (ENISA), via updated Memoranda of Understanding (MoU).
- We will build on existing initiatives such as the [Internet Privacy Engineering Network \(IPEN\)](#) and consolidate the network for technology expertise among data protection authorities in Europe. We aim to develop core knowledge on how essential and emerging technologies work. This will include talking to innovators in the private sector.
- We will invest special attention to the development of eHealth services at EU level.
- We will develop a consistent and targeted communications strategy with various stakeholders to address the COVID-19 pandemic’s newest developments and data protection issues. In 2022, we will host a conference on how to safeguard individuals’ rights in a world that will, hopefully, be recovering from this current crisis.

Action

EDPS to support EUI to continue to lead by example in safeguarding digital rights and responsible data processing.

2.1 Tools

We are going to use the tools we have and develop new ones

Privacy and data protection are cornerstones in any democratic society based on the rule of law and fundamental rights. Likewise, a free internet society depends on the design of technology. This is particularly relevant whenever the EU adopts laws and policies related to the processing of personal data, or when EUI process personal data.

Personal data have and will continue to play an important role in the fight against the COVID-19 pandemic. Our laws, such as the GDPR and the ePrivacy rules, allow for the processing of personal data for public health purposes, including in times of emergency. Data protection law is well-equipped to help support the public good, and do not represent an obstacle, in fighting the virus. It is certainly possible to build technological solutions, which are compliant with the legal data protection framework. Some recent application show that societies can take up technologies while upholding privacy and data protection rights. It remains paramount that EUI and Member States continue to actively engage with DPAs.

Certain processing activities are however, by their nature, highly risky, they may even violate the essence of fundamental rights and freedoms and should be suspended or stopped altogether, i.e. when broad internet content monitoring interferes with privacy and freedom online. Being a supervisory authority, we must be equipped to monitor and anticipate problems and quickly respond to operational situations, policy and legal questions. We recognise DPOs'of EUI as the emissaries of positive change in how data is handled.

The outsourcing of tasks by EUI to providers of communications services and digital tools is an operational reality, and often a necessity. This, however, creates risks for data protection and good administration, particularly where there are few or no viable alternatives to monopoly providers with questionable standards on privacy and transparency.

The EU and European public administrations have considerable leverage to bring about real change to business models which are not consistent with EU values, fundamental rights and data protection rules. This was particularly relevant when an enforcement action was launched in 2019 concerning EUI contracts with software providers. There is now a renewed appetite for coordinated support to the European industry and for data to be processed according to our European values.

In this sense, our commitments are as follows, we will:

- Promote data protection by design and by default, to be implemented irrespective of the technology deployed or the political priorities.
- Develop effective oversight mechanisms, particularly on technologies and tools, when these are deployed in the common fight against COVID-19, to empower and not control, repress or stigmatise citizens.
- Contribute to developing strong oversight, audit and assessment capabilities for technologies and tools, which are increasingly “endemic” to our digital ecosystem

(e.g., profiling, machine learning, AI). We will provide guidance on personal data processing using automated decision-making systems and AI.

- Support the idea of a moratorium on the deployment, in the EU, of automated recognition in public spaces of human features, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, so that an informed and democratic debate can take place.
- Reinforce the central role of the controller in relation to [processors](#) and sub-processors in EUI, both by raising awareness and, more formally, by providing advice on possible standard contractual clauses.
- Aim to minimise our reliance on monopoly providers of communications and software services, to avoid detrimental lock-in and work with other EUI and other public administrations in the EU so they can do the same. We will call on EUI and other public administrations in the EU to review their external contracts on digital products, software, services and technology to achieve compliance as required by EU data protection laws. We will explore how to deploy free and open source software and solutions.
- Review previous authorisations for transfers to third countries and adopt standard data protection clauses.
- Continuously assist EUI by demonstrating and developing bespoke privacy tools and solutions. This also involves giving advice when [Data Protection Impact Assessments \(DPIAs\)](#) are necessary.
- Publish standardised information about personal data breaches that are notified to us, including the types of organisations involved and the number of people affected.
- Use our enforcement powers to ensure EUI websites and mobile apps are complying with EU law, particularly in respect of third party tracking.
- Closely monitor the ongoing process that makes EU systems ‘interoperable’, with a particular focus on the access and processing of personal data (Europol, Frontex et al.), in collaboration with national supervisory authorities where needed, to ensure effective supervision.
- Launch, explore and explain, as a follow up to the ‘[Necessity Toolkit](#)’ and ‘Guidelines on [Proportionality](#)’, the concept of the ‘essence’ of the rights to privacy and data protection, based on the jurisprudence of the Court of Justice and growing scholarship in this area.

2.2 Coherence

We do not protect data - we protect human beings

The GDPR is directly applicable throughout the EU. Nevertheless, it provides Member States with the possibility to further legislate their respective laws. This could compound the fragmentation of national approaches. The EDPB exists to check and avoid such fragmentation.

The EDPS has a unique dual role as a full member and provider of the EDPB's secretariat. We will exercise this role creatively, seeking to represent the wider EU interest, and contribute to the success of the EDPB, as well as ensuring the consistent application and enforcement of the GDPR and [the Data Protection Law Enforcement Directive](#). We aim to develop with other DPAs a common set of tools.

The EU has not completed its updating of the data protection framework for the digital age. EU legal gaps remain, where specific data protection rules are either absent – for the processing of personal data by the Common Foreign and Security Policy (CFSP) mission as referred to in [Articles 42\(1\), 43 and 44 TEU](#), or fragmented police and judicial cooperation in criminal matters, as well as Europol and EPPO. Such a situation undermines the possibility of achieving a consistent approach to protecting individual's personal data in the EU. We will interpret the applicable rules in the spirit of the EDPR, and we will apply the principles of the Regulation in areas where specific rules are missing.

We need up-to-date - but also technologically neutral - rules on the protection of [confidentiality](#) of electronic communications. Sustainable economic growth cannot be achieved through the infinite monetisation of people's private conversations or indiscriminate retention of all communications data.

Personal data supports privacy, as well as other rights and freedoms, such as freedom of expression and non-discrimination. We recognise the synergies between the enforcement of data protection and other rules applicable to the digital economy, especially concerning consumer and competition law, and will carry on our work to ensure that they are mutually reinforced.

EUI are already making use of new and emerging technologies. In the interest of a coherent approach throughout the EU, the EDPS recommends that any new EU regulatory framework, such as potential AI, will apply both to EU Member States and to EU institutions, offices, bodies and agencies.

Data protection and privacy are the foundations for democracy in a time of digitisation. To this end, we will:

- Continue to build the capacity of the EDPB, both as a member and as a provider of its secretariat, to ensure that, by 2025, the GDPR is recognised as a model for all democracies around the world - a formidable blueprint to strengthen the trust and respect in the digital society.
- Call for a stronger expression of genuine European solidarity, burden sharing and common approach to ensure the enforcement of our data protection rules. The EDPS supports the establishment of a Support Pool of Experts within the EDPB, which would assist DPAs dealing with resource-heavy and complex cases.
- Contribute to the review of Regulation (EU) 2018/1725, scheduled for April 2022, and make a strong case to address the gaps and discrepancies that continue to exist. In the meantime, the EDPS will interpret any specific rules in the spirit of Regulation (EU) 2018/1725.
- Closely monitor the use of new tools involving data analytics and artificial intelligence by Europol and other agencies in the AFSJ, in compliance with the

mandate assigned to them by law, while promoting solutions to protect individuals' rights and freedoms.

- Call for a coherent approach regarding new EU regulatory frameworks on the use of new technologies so that EUI are subject to the same rules as those applied in EU Member States.
- Supervise EPPO as new actor in the criminal justice area, and especially its relations with Europol and Eurojust.
- Call for the adoption of the proposed ePrivacy Regulation, but not to the detriment of existing protections.
- Contribute to the establishment of the Digital Single Market where European rules on privacy and data protection, as well as competition law, are fully respected. We will also make sure that the rules on the access and use of data are fair, practical and clear.
- Develop European and international cooperation measures, and promote joint enforcement actions and active mutual assistance, by concluding - when necessary - Memoranda of Understanding with DPAs.

Solidarity

The EDPS promotes a positive vision of digitisation that enables us to value and respect all individuals. The full potential of data shall be dedicated to the good of society and with respect to human rights, dignity and the rule of law.

3.1 Justice

We actively promote justice and the rule of law.

Solidarity, being aware of shared values, interests and objectives, is at the heart of the EU project. As an EU institution, the EDPS is committed to upholding the rule of law and democracy. As an independent data protection supervisory authority, we act in line with these values. When we believe that these are threatened, we speak up, and vigorously defend them. Likewise, we take action if the independence of other DPAs and the 'collective independence' of the EDPB are jeopardised.

When planning strategies on democracy and human rights, the EU should promote digital justice and privacy for all. Privacy and data protection can never be traded for access to essential services. Data protection is one of the last lines of defence for vulnerable individuals, such as migrants and asylum seekers approaching EU external borders. Although the EU has accumulated a patchwork of measures in the areas of police and judicial cooperation and border management, the legal framework remains fragmented, creating unnecessary discrepancies. This puts unwarranted constraints on the EDPS' supervisory and enforcement powers.

Fundamental rights are necessary because they protect those less likely to have the means to fully defend themselves. In the so-called gig economy, workers and consumers

find themselves governed by algorithms that make decisions based on data collected about them, with limited ability to understand or challenge those decisions. Women, people of colour and those with disabilities are routinely discriminated against, and this is reinforced by the proliferation of algorithmic decision-making.

We recognise the need for individuals to have greater control over whether data about them is collected, and, if so, how and for what purpose their personal data is processed. Where the digital environment becomes more complex, responsibility falls on controllers and enforcers to avoid any data practices that harm the rights or interests of the individuals concerned. The burden of proof should not fall on those individuals to understand risks and take action.

In complex scenarios, '[consent](#)' should not be relied upon because it indicates obvious power imbalances between the controller and the individual's rights to data protection. We are convinced that EU data protection legislation provides other lawful grounds for processing.

A misguided debate continues on the appropriateness of the concept of personal 'data ownership'. This is unlikely to be compatible with the Charter of Fundamental Rights and will not empower individuals in a digitised society. We believe data protection 'disrupts' the markets for personal data, where data as a commercial or political asset is monetised or used to manipulate people. DPAs acting collectively should be an agent for such positive changes.

In this context, we will actively:

- Stress that privacy and data protection are an integral part of the rule of law and can never be treated in isolation. We will take actions if the independence of other DPAs or the 'collective independence' of the EDPB are jeopardised.
- Advocate for the fundamental rights to data protection and privacy to be at the heart of the Conference on the Future of Europe. We will also support the efforts to integrate data protection considerations in the [European Democracy Action Plan](#), as a safeguard for independent journalism, lawful dissent and political activism.
- Continue to enforce EUI compliance with the rules, to protect those who are in a position of weakness, such as minors or displaced persons near or at the EU's external border. Indeed, they have as much of a right to data protection and privacy as anyone else.
- Identify discrepancies in the standards of data protection within EU law in the Areas of Freedom, Security and Justice (AFSJ) and we will consistently enforce the rules.
- Encourage the European Commission to further harmonise the data protection rules on processing operational data (Chapter IX of the Regulation 2018/1725), including in the context of the [Europol Regulation](#) review
- Advise EU lawmakers to safeguard data protection and privacy in [the New Pact on Migration and Asylum](#).

- Keep contributing to the European Commission’s proposals related to combatting discrimination.
- Provide guidance to EUI on policies and measures (such as the [Digital Services Act](#)) that hold private companies accountable for manipulation and amplification serving private gain, but to avoid blanket monitoring and censorship of speech that inevitably interferes with the rights to privacy and data protection.
- Building on our experience with the [Digital Clearinghouse](#) and other fora, we will work with the EDPB, the European Commission and the relevant EUI to establish practical cooperation and joint enforcement between digital regulators on specific cases and learn lessons from the past.
- Actively contribute to the development of a common EU vision on digitisation and technology. For example, determining how AI can be used for humankind and re-engineered along the lines of EU rights and values and alongside strict liability rules; so that manufacturers and controllers are held responsible for damage caused by defects in their products, even if the defect resulted from autonomous decisions after its entry on the market. In the interest of a coherent approach throughout the EU, the EDPS recommends that any new regulatory framework should apply to both EU Member States and EUI. Where EUI use AI, they should be subject to the same rules as those applied in EU Member States.
- Regularly engage in the debate on digital ethics, emphasising the need to not only comply with the law, but to also consider the effects of data processing by controllers in EUI and elsewhere, on individuals, groups and society; including shared values and the environment.
- Promote diversity in all discussions on data protection, including those we organise ourselves. We will ensure gender balanced representation among speakers and panellists in the conferences or events we organise.

3.2 Sustainability

We know there is only one world

Data processing and data protection have to go green.

The EDPS is a socially-responsible organisation. Our values are to treat people – our employees, the people whose activities we supervise, the individuals whose data is processed by EUI, our stakeholders - and the natural environment around us, with respect.

The ongoing development of AI and blockchain based technologies, as well as illegal tracking and profiling of individuals generate an increasing amount of dangerous waste, due to short-lived connected goods, combined with exponential carbon footprint emissions. This is a great source of concern in light of the [EU Green Deal](#) and data protection in this new decade.

Enforcing personal [data minimization](#) and responsible data processing can be part of the solution to help counteract these damaging trends. There should be competition on the most beneficial ways to use data, not on who can collect the most.

The redistribution of wealth and its practical application are bound to change with the continuous evolution of social norms, politics, and culture. As highlighted by [the EDPS' Preliminary Opinion](#) on scientific research and data protection, there is growing concern about how digitisation has contributed to the exponential growth in data generation; while also concentrating the control of the means for converting that data into valuable knowledge in the hands of a few powerful private companies. There are growing calls for regulated access across the EU to privately-held personal data for research purposes exclusively serving the public interest to improve health care, advance health research and address the climate crisis or growing social inequalities. While the [Open Data Directive](#) organises the access to public sector information to foster competition and economic innovation; access to privately held data by non-profit stakeholders to foster social and solidarity innovation and scientific research in the public interest deserves specific attention as well. Current barriers to such access reveals the need for a broader debate on a data redistribution policy for the digital age, to maximise societal benefits of data sharing initiatives, in compliance with the European fundamental rights framework. To address these challenges, we will:

- Convey a deeper understanding of the impact of digitisation on our world.
- Encourage broader and long-term view of the future of data protection in a period of environmental crisis, growing inequalities and geopolitical tensions.
- Pay particular attention to our energy consumption, emissions due to the travelling of officials (missions), procurement and commuting to and from work, promoting telework.
- Engage in the debate on data sharing to advocate for a data redistribution policy for the digital age based on a rigorous proportionality tests and appropriate safeguards - including anonymisation and pseudonymisation - against misuse and unlawful access.