21 December 2021

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

"Contribution by the European Data Protection Supervisor to the Report on the application of Regulation (EU) 2018/1725, the EUDPR"

Contribution by the European Data Protection Supervisor to the Report on the application of Regulation (EU) 2018/1725, the 'EUDPR'.

Key messages

Regulation (EU) 2018/1725 (EUDPR) is the data protection regulation for EU institutions, bodies, offices and agencies (EUIs), which entered into force in 2018.

The application of the EUDPR has been an undeniable success. Similar to the General Data Protection Regulation (GDPR), the entry into force of the EUDPR represented a key moment for the protection of the fundamental right to data protection in the EU.

Individuals whose data is processed by EUIs now benefit from the same level of protection as ensured by the GDPR. This means that individuals dealing with any EUI know that their rights can be effectively enforced, thanks to the greater clarity of the applicable rules. Most importantly, the investigative and sanctioning powers explicitly attributed to the competent supervisory authority, the European Data Protection Supervisor (EDPS) reassure individuals that compliance with data protection rules is taken seriously.

The European Commission is now preparing its report on the application of the EUDPR according to Article 97 of this same Regulation.

With its first-hand experience of applying and enforcing the EUDPR, the EDPS is happy to contribute to this important reviewing exercise.

The EDPS also notes that under Article 98 of EUDPR, the Commission has to present by the same deadline as foreseen in Article 97 a review of the legal acts regulating the processing of 'operational personal data' by EUIs when carrying out activities falling within the scope of Judicial cooperation in criminal matters[1] and Police cooperation[2].

Given the EDPS' role and experience in supervising EUIs' processing of personal data in the aforementioned fields, the present contribution also contains relevant considerations on the rules on the processing of operational personal data which could feed the review process in this sector. Reviewing the application of the EUDPR in relation to this sector is of particular importance considering that objective of fighting crime, albeit important, should not lead to disproportionate interferences with the fundamental rights to privacy and data protection of persons dealing with EUIs.

Concerning the rules applicable to personal data and to operational personal data in general, the EDPS is convinced that the current legal framework is capable of delivering the expected outcome in terms of protection, if effectively applied and enforced.

The EDPS also attaches the utmost importance to its consultative function and its role as trusted advisor to the European Commission, the Council and the European Parliament on the many legislative and non-legislative proposals, or other initiatives

[1] Chapter 4 of Title V of Part Three TFEU.

[2] Chapter 5 of Title V of Part Three TFEU.

affecting the rights to privacy and data protection. The EDPS welcomes the clarity brought by the provisions which confer upon it an advisory role on draft legislative or administrative measures prepared by EUIs with an impact on the right to protection of personal data. The EDPS also welcomes and encourages the informal cooperation and the open dialogue with all EUIs that often precedes and prepares its formal consultation on such acts and measures mandated by Articles 41 and 42 of the EUDPR.

Nevertheless, this contribution identifies several provisions that might still benefit from clarifications from the legislator, in particular with regard to the processing of operational personal data. The EDPS is not of the opinion that amendments to the EUDPR and to the acts referred in Article 98 are required urgently.

In particular, the EDPS believes that the legislative framework enables it to ensure appropriate supervision, including deployment of its corrective powers, to all situations of processing of personal data by all EUIs, including in the Area of Freedom, Security and Justice.

It should be acknowledged, though, that in the three years of application of the EUDPR, the experience with enforcement is still at its early stages and enforcement problems, including those stemming from diverging interpretations of the rules and their remaining fragmentation across various instruments, cannot be excluded.

A specific mention should be made regarding the provisions of Chapter VII of the EUDPR on cooperation and their interaction with the corresponding provisions in Chapter VII of the GDPR. Given the scope of the supervision entrusted to the EDPS by the legislator, covering processing by EUIs, effective cooperation with national Data Protection Authorities (DPAs) in charge of supervising entities subject to the GDPR, but acting on behalf of EUIs (e.g. as processors for EUIs), is essential to ensure effective enforcement of data protection rules related to EUIs. In other words, such cooperation is essential to ensure the effectiveness of the provisions of the EUDPR.

The EDPS notes that, in particular thanks to the coordination role of the European Data Protection Board (EDPB), it is possible to interpret the provisions of chapters VII of both the GDPR and the EUDPR, so as to ensure seamless protection of personal data processed by EUIs, when such data is processed directly and when it is processed on behalf of the EUIs. However, early experience shows that concrete problems may arise, and that the suitability and the functioning of the provisions on the cooperation between the EDPS and national DPAs should be closely monitored and reassessed, if necessary.

Lastly, concerning the production of legislation having an impact on personal data protection, on which the EDPS will be called to formulate its Opinions, is likely to grow under most imaginable scenarios. Draft legislation currently being discussed confers additional tasks to the EDPS. The stepping up of effective enforcement actions that underlies the adoption of the EUDPR is ongoing, occurring within an increasingly complex legal and technical landscape. These trends expose the fact that the success of the EUDPR hinges on the EDPS being adequately equipped in terms of resources to fulfill all its tasks under the EUDPR.

The EDPS will always incorporate in its activities the consideration that protection of personal data and the protection of privacy are not ‘absolute’ rights. As such, the EDPS will always try to fully apprehend the need for EUIs to conduct their tasks in the pursuance of their objectives and more generally in the overall interest of the EU.

Having said that, the EDPS will not hesitate to take action when necessary and expects from EUIs a culture of compliance well-embedded in their daily work.

In the sections that follow, the EDPS provides answers to the questions received by the Commission to help prepare its report on the application of the EUDPR. The questions are based on those asked to national DPAs as part of the 2020 GDPR evaluation. Where relevant, the EDPS has provided additional information to accompany the responses to the questions raised by the Commission. In doing so, the EDPS hopes to provide more transparency and greater insight into its practical experiences when carrying out its tasks under the EUDPR.

CLUSTER 1: THE EDPS AS SUPERVISOR OF EUIS

1) **Concerning consultations from the EUIs regarding operational questions of EUDPR compliance (i.e. consultations other than Art. 42 legislative consultations – for them, please see below on question 8), please provide the following information:**

Introductory remarks

The statistics below cover the consultations to which the EDPS replied either informally at staff level or through an opinion signed either by the Supervisor or the Head of Unit. In addition to these consultations that are registered in our Case Management System and result in a written opinion, the EDPS answers numerous questions from Data Protection Officers (DPOs) concerning processing operations, data protection obligations, or data protection concepts. Such questions are received via emails or telephone to EDPS staff members or to the EDPS' DPO hotline. These questions are of very informal nature and may not be registered as separate consultation cases.

In general, following the *Schrems II* judgement, supervision activities relating to international transfers became particularly significant. A first prior consultation falling within the scope of Article 40 of the EUDPR from the European Central Bank regarding the software 'Microsoft Dynamics 365' and associated transfers required an in-depth assessment within the deadline set by the Regulation and involved the use of the EDPS' corrective powers (issuance of a warning under Article 58(2)(a)). The EDPS also authorised temporarily, under Article 48(3)(a) of the Regulation, the use of *ad hoc* contractual clauses between the Court of Justice of the European Union and the company, 'Cisco', for transfers of personal data in the context of recourse by the Court to the 'Cisco WebEx' application and related services.

Besides, EUIs have also started to request prior authorisations to conclude administrative arrangements under Article 48(3)(b) concerning transfers between EUIs and non-EU/EEA countries' public authorities. The EDPS has already assessed and authorised, under certain specific conditions, three administrative arrangements. This trend will likely continue in the future.

On his initiative, the EDPS has also conducted an assessment of high-risk transfers carried out by EUIs and opened two investigations, one regarding the use of cloud services provided by Amazon Web Services and Microsoft under the procurement

procedures of the EUIs, and one regarding the use of Microsoft Office 365. In order to ensure homogeneous interpretation of the GDPR and the EUDPR, staff members involved in supervision activities are also increasingly involved in EDPB work, including the first coordinated action under the "EDPB Coordinated Enforcement Framework" on the use of cloud based services by the public sector.

The EDPS has also been consulted informally and formally on a wide range of novel issues involving the processing of personal data for the fight against the COVID-19 pandemic, leading the EDPS to issue detailed Orientations and Guidelines for the benefit of all EUIs.

a) Numbers of consultations received and answered (distinguishing between types of consultations) in 2018, 2019, 2020, 2021.

	2018	2019	2020	2021
Consultations	50 (*only 2 were issued after the entry into force of EUDPR*)	75	59	52
Prior consultations	0	0	1 (inadmissible)	4 (including 1 inadmissible)
Transfer authorisations	0	1	0	4

b) If statistics are available: what percentage concerned "administrative" processing operations (HR, budget…) and core business activities, respectively (if no statistics available, please provide an estimate of the split and whether it has changed compared to the old Regulation (EC) 45/2001)?

While a majority of supervision activities still focus on administrative procedures within EUIs, the digitalisation of EUIs' internal and external communication, as well as some of their core business activities has increased dramatically EUIs' reliance on ICT providers. This trend is therefore accompanied by a shift from the supervision of administrative files to core business files[3].

	2018	2019	2020	2021
Consultations	28% core business	21% core business	27% core business	20% core business
Prior consultations	N/A	N/A	100% core business	50% core business

[3] Several consultations relate to the interpretation of a provision of the EUDPR or the implementation of a provision of EUDPR that are either of a general nature and not necessarily related to either administrative procedures or core business processing (ex: interpretation of Article 39 on the need for a Data Protection Impact Assessment) or relevant to both administrative procedures and core business activities (ex: Art. 25 on restrictions to data subject rights when not related to a specific area - There were a significant number of those in 2019, 2020 and 2021).

2) **Regarding complaints by data subjects:**

a) **How many complaints did you receive in 2018, 2019, 2020, 2021?**

Year	Complaints received	Admissible	Inadmissible
2018	298	58	240
2019	210	59	151
2020	246	43	203
2021 (latest update 15 Nov 2021)	313	44	269

b) **How many decisions on complaints did you issue in 2018, 2019, 2020, 2021? If available, please provide a breakdown of the outcome: infringement found (incl. of which Article of EUDPR) / no infringement found / inadmissible.**

Year	Decisions[4] on admissible complaints
2018	23
2019	48
2020	35
2021	22

Complaint cases present different degrees of complexity and while some can be handled swiftly, certain require an in-depth analysis and involvement of several colleagues (including colleagues with technical expertise). Investigations are often time-consuming and complex, therefore demanding several rounds of exchange of views and fact-finding exercises before the EDPS is in a position to adopt a decision.

Furthermore, it is increasingly common for both EUIs and complainants to request a review of our decisions. Preparing the reply to such requests requires a thorough assessment of the elements put forward; a work which is carried out under certain time pressure, bearing in mind the legal deadline to challenge our decisions before the General Court.

It should also be noted that many cases remain open for long periods of time because of their complexity, the volume of documents, the responsiveness and degree of cooperation of complainants and of EUIs, the existence of parallel administrative or judicial procedures which warrant the EDPS to suspend the

[4] 'Decisions' include also cases closed by amicable settlement, referral to the DPO and other means of closure.

investigation, and, of course, the workload of EDPS case handlers. To date, there are approximately 65 complaint cases which remain open, i.e. for which no decision has yet been taken.

NB: For inadmissible complaints[5], the EDPS does not issue decisions, but replies to the complainant, directing them to the relevant authority. A complainant may however request that the EDPS reviews such a reply, lodge a complaint with the European Ombudsman, or an action before the Court of Justice contesting the inadmissibility of the complaint (e.g. for lack of EDPS competence).

3) Regarding inspections/audits[/investigations]:

The EDPS has both an audit function and an investigation function.

The staff in charge of the audit function draws up and executes an annual audit plan and advises EUIs in light of the results of this plan.

The staff in charge of investigations makes its inquires when there are suspicions that the Regulation has been infringed with a view to exercising the EDPS' corrective powers.

Our responses under this point cover audits and investigations in turn.

a) How many inspections/audits did you carry out in 2018, 2019, 2020, 2021?

The following audits and inspections were carried out by our audit function.

2018	5
2019	9
2020	4
2021	4

The following formal investigations were launched by our investigations function.

2018	-
2019	4
2020	1
2021	2

[5] Inadmissible complaints are those that concern processing operations carried out by entities which are not EUIs and therefore do not fall under the EDPS' supervision, such as national authorities or private companies.

b) How do you choose which processing operations to audit [and investigate]?

Audits

As outlined in the respective EDPS policy document, circumstances triggering the conduct of audits can be identified during the various internal activities of supervision and consultation within the EDPS, but they can also come from external sources, such as the media. It is important to note that audits can be triggered by a *combination of factors*, which, when considered together may potentially indicate serious issues or failings within the EUI concerned. A fraction of targeted institutions is determined by the drawing of lots.

Based on the Annual Audit Plan, EUIs may be chosen for general, targeted audits. The Annual Audit Plan is based on the results of a risk analysis of all EUIs, and also takes into account resource limitations and budget constraints. Any audits which the EDPS has a legal obligation to carry out (in the area of large scale IT systems) will also be reflected in the Annual Audit Plan, but will not be included in the risk assessment exercise.

The risk assessment exercise is based on specified risk factors (criteria) that may indicate serious compliance issues or failings within the institution concerned. In particular, these refer to information on the:

- nature and number of consultations submitted and/or Data Protection Impact Assessments (DPIAs) performed, in particular when sensitive data is processed as a core business, or when recommendations made qualify for on-the-spot verifications;
- possible transfers of data to recipients who are not subject to the GDPR;
- increase in admissible complaints received by the EDPS;
- justified recommendation made by a case officer to carry out an audit;
- results and date of the last audit/visit.

Due to the COVID-19 crisis and the restrictive measures with an impact on how the EDPS has had to carry out its work, the Annual Audit Plan 2020, and the Annual Audit Plan 2021 are based on a selection of remote audits on specific topics rather than audits carried out as a result of the aforementioned risk assessment exercise. For these remote audits, criteria guiding the selection of audits were:

- the impact on and number of individuals concerned;
- the number of EUIs covered; as well as
- the likelihood of lessons learned as a result.

Investigations

The choice of targets for investigations also reflects the EDPS' institutional priorities. In 2021, the two investigations we launched formed the enforcement pillar of the EDPS' strategy for EUIs to comply with the *Schrems II* judgement.

4) Which corrective powers did you use since the entry into application of the EUDPR? Please provide statistics.

Type of corrective power by reference to Article 58(2) EUDPR	**Number**
Article 58(2)(a)	2
Article 58(2)(b)	5
Article 58(2)(e)	2
Article 58(2)(g)	1

58(2)(a): Prior consultation on ECB's Customer Relationship Management system.

Our opinion on the ECB's proposed use of Microsoft Dynamics 365 (see our response to question 1(b) above) resulted in the issue of a warning pursuant to Article 58(2)(a) of the EUDPR that the envisaged processing operation was likely to infringe the regulation. We made a number of recommendations to assist the ECB in ensuring compliant processing.

58(2)(b) and (e): EDPS investigation into the European Parliament's use of Nationbuilder. We investigated the Parliament's use of a US-based political campaigning company, 'Nationbuilder', to process personal data for its 'thistimeimvoting.eu.' website, in the context of the 2019 Parliamentary election. The EDPS ordered the Parliament to publish a data protection notice - complying with the EUDPR - on its website. The Parliament failed to comply with this order, which led the EDPS to issuing a reprimand. We further issued several recommendations; the Parliament acted in line with them. In November 2019, the EDPS visited the Parliament to confirm the deletion of 260,000 users' personal data who had not accepted the updated policy.

58(2)(e): EDPS investigation into the European Parliament's Wi-Fi. The EDPS found a significant issue regarding the definition of personal data processing, which consequently had an impact on the transparency of the processing and the information to be provided to individuals. The EDPS issued an order requesting the EP to publish an updated and compliant data protection notice. We further issued several recommendations. The Parliament acted in line with the order and the recommendations. The investigation was carried out in 2020; a final decision based on its findings was issued in 2021.

58(2)(g): EDPS consultation on the use by the European Asylum Support Office (EASO) of social media monitoring. On 30 September 2019, we issued a temporary ban on the production of social media monitoring reports by EASO. This decision was made because EASO was using the social media monitoring reports to give management and relevant stakeholders news on the latest shifts in asylum and migration routes and smuggling offers, as well as an overview of conversations in the social media community relating to key issues, such as flight, human trafficking and other asylum systems and processes. EASO was doing this without the necessary legal

basis. We verified that the ban had been implemented when we visited EASO in November 2019.

The rest of the cases concern complaints against several EUIs. Decisions following complaints are not published.

Investigative powers achieve an important, albeit, indirect 'compliance effect' which is also worth flagging in this section.

For instance, the EDPS issued an order to EUIs to provide information about certain categories of their international transfers of personal data. This order had a great effect on ensuring compliance. It allowed the EDPS to map out international transfers of personal data performed by EUIs and develop his strategy for EUIs to comply with the *Schrems II* ruling.

5) Do you also use other tools such as recommendations or "amicable settlements" to ensure compliance? Do they reliably work to obtain compliance?

When the complaint can be solved with an investigation (for instance, where a complainant has not been granted access to their personal data, but the EUI grants access to this data once the EDPS intervenes), the EDPS will typically not issue a decision, but simply inform the complainant (and the EUI) that since the their request has been satisfied, the case will be closed. Should the complainant believe that their concerns have not been fully addressed, the EDPS will assess whether there are reasons to pursue the investigation. Amicable settlements are an efficient way of solving cases which stem from administrative oversights, such as the EUI not replying to individuals' access request in time. Like the other supervisory authorities, the EDPS does not consider amicable settlement possible nor appropriate in other types of cases, e.g. own initiative inquiries/investigations.

Complaint decisions can include recommendations to the EUI, typically where no violation has been found, or corrective powers would not be considered proportionate in relation to the violation found. Recommendations can be used in case the EDPS believes that there is room for improvement in the EUI's practices (for instance, amend a data protection notice to make it clearer). Similarly, the EDPS can also issue recommendations in other types of cases, e.g. inspections/audits, prior consultations, own initiative inquiries/investigations, to improve compliance with the EUDPR.

6) Please provide statistics on data breach notifications received in 2018, 2019, 2020, 2021. Please provide statistics on follow-up given and the time it took to provide follow-up.

Since the entry into operation of the obligation for EUIs to notify personal data breaches to the EDPS, the EDPS has received an ever-growing number of personal data breach notifications.

The **number** of notifications received (with a breakdown on whether these were provided "in phases") is provided below:

Numbers of Data Breach Notifications	Total	Comprehensive	In Phases
2018	7	5	2
2019	95	55	40
2020	121	68	53
2021	82 (until mid November)	47	35

With regard to the **type** of personal data breaches, the vast majority of cases concerned confidentiality breaches (1-2 cases per year concerned availability or integrity of personal data).

Regarding the **root cause** of personal data breaches, the majority of personal data breach cases notified to the EDPS were due to human error.

The most common examples include, sending an email to the wrong recipients or putting all recipients in copy whereas their contact details were not to be disclosed to the rest of the recipients list. The EDPS also received data breach notifications concerning documents that were published on EUIs' websites as part of the access and transparency procedures without removing personal data. The COVID-19 crisis has also contributed to personal data breaches caused due to human error, as employees could not access certain tools and therefore had to carry out certain tasks, which involved the processing of personal data, manually when teleworking (e.g. tool for mass emailing not accessible outside premises). Several personal data breaches concerning erroneous revelation of personal data in the context of EUIs' COVID-19 contact tracing process were also notified to the EDPS.

Root cause	Human error	External attack	Technical error
2018	5	1	1x
2019	62	9	13
2020	63	21	25
2021	48	16	12

Technical errors were the second cause of personal data breaches. Technical errors occur when personal data were made accessible to unauthorised users. The most common type of error concerns the provision of access to documents containing personal data that one should not have access to.

The third most common root cause of personal breach are external attacks.

Such external attacks are on the rise, especially after the start of teleworking patterns due to the COVID-19 crisis. These attacks usually affect larger numbers of individuals, compared to data breaches that occur because of human error. External attacks typically allow access to full databases or systems, in which data about different individuals are stored.

Other root causes of personal data breaches include abuse of privileged accounts to access personal information and theft or loss of documents and devices.

The handling of personal data breach notifications received from EUIs requires significant effort and human resources from the EDPS. A detailed assessment has to be undertaken for every case; in complex situations, significant amount of documentation is needed and meetings have to be organised with the controller.

The following numbers represent the **closed cases** in the registry of the EDPS. This number is indicative as some cases are still ongoing. In addition, several controllers that have sent a notification have not concluded the notifications' procedures in most cases. In some cases, the EDPS has not yet handled the data breach notification.

Year	**Closed cases**
2018	7
2019	59
2020	16
2021	13

When a notification of a personal data breach by an EUI is received, the EDPS sends an immediate notification of acknowledgement of receipt, usually within 48 hours. The EDPS also aims, within the first 48 hours, to primarily assess the risks to individuals' personal data and, if necessary, either asks for further information, or provides advice to data controllers about the immediate measures they should take. Advice given may include informing the affected individuals in case of high risk **(follow-up)**. There are no rules concerning the deadlines to close personal data breach cases as the time required to handle the data breach also depends on the time the controllers will need to investigate the incident and provide follow-up information. This is particularly relevant in cases of external attacks, as the forensic investigation on the controller's side may take a long time.

The EDPS also receives **notifications outside its competence**. In2021, we received 6 notifications that were sent from private companies or individuals (whistleblowers) outside the scope of application of the EUDPR. These were either from companies having a main establishment in the EU (where the national DPA according to the GDPR would be competent) or from companies processing personal data of EU citizens, without being established in the EU. In the first cases, the EDPS notified the controllers and provided relevant contact information for the national DPA. In the latter cases, the EDPS will send a reply indicating its lack of competence.

7) **Please provide information on training / awareness-raising activities provided to the EUIs (so excluding events targeted at audiences outside the EUIs):**

a) **what was the number of sessions organised in 2018, 2019, 2020, 2021 and what was the numbers of participants; if no statistics are available, please provide estimates:**

Year	Number of events	Number of participants
2018	14	Estimate more than 1000 participants
2019	34	Estimate more than 4600 participants
2020	21	Estimate more than 1700 participants
2021	23 (until 15 November 2021)	Estimate more than 1800 participants

b) **Please provide an overview of topics covered (e.g. via titles of presentations).**

Between 2018 and now, the EDPS, and more specifically his staff in charge of supervision and enforcement activities has invested a significant amount of resources in providing training to data controllers, DPOs, and, more generally; to EUI's staff. The EDPS has been giving once a month, a 2-hour training to EU staff who attended the lunch conferences organised by the European School of Administration. The training sessions focused on the new obligations, highlights and rights under the EUDPR. Since the end of 2019, the EDPS has also been providing thematic training sessions at European School of Administration, on topics of particular relevance or interest for EUIs, namely on data protection aspects in public procurement; data protection in events management; joint controllership; personal data breaches; and (international) transfers.

Moreover, the EDPS has provided many training sessions to various EUIs upon request from their DPO (e.g. Directorate-Generals of larger EUIs, Executive Agencies, decentralised Agencies).

In 2020 and 2021, most of the training sessions were carried out remotely. In April 2021, the EDPS prepared a 2,5h online training session with an external contractor, which entailed a 5-month investment. The course is now available on the EU-LEARN application and EU staff can follow it at any time.

The title of presentations delivered can be found in **Annex I.**

A list of training sessions delivered between 2018 and 2021 can be found below.

2018

1. February 2018 ERCEA (>70 participants) Personal Data breaches Seminar
2. 22 March 2018 "Data protection reform Security Related Aspects" to European Commission LISO Officers
3. On 26 January 2018, webinar to CEPOL LE Directive on the new Regulation and IT issues: 30 staff

4. On 31 January a 2 hour training to the Ombudsman on how to get ready for the new Regulation: 40 staff
5. On 30 and 31 January at ECA, EC, EP, CJEU, EIB, EIF, CHAFEA, CDT trainings on accountability and the new Regulation:100 participants
6. On 2 and 3 March 2018 trainings and case studies to 70 staff at ENISA
7. On 16/02/18, 16/03/18, 04/05/18, 02/07/18, 12/9/18 and 4/10/2018, 2-hour trainings at EUSA on the new Regulation and how to get ready: 300 participants in all sessions
8. On 7 June 2018, a 2 hour training to DGs CLIMA and MOVE on the new obligations of the Regulation: 60 staff
9. On 14 June 2018, a webinar to 100 participants of the CEIII Social Media Group how to apply the new Regulation on online communications
10. On 18 September 2018, a presentation to Web Managers Network on web, social media and new data protection rules: 70 participants
11. On 20 and 21 September 2018, trainings and workshops on the new Regulation at the ETF, Torino: 70 staff
12. On 1st and 2nd October 2018, 2 full day trainings with case studies to 100 participants from the CJEU, EP, COM, CdT, ECA, Luxembourg
13. On 7 November 2018, at DG FISMA on the new Regulation and case study on events management
14. On 3 December 2018, a presentation to DG COMM on the data protection reform for managers

2019

1. 4 April 2019 EDPS / the European Union Agency for Network and Information Security (ENISA) workshop “Towards assessing the risk in personal data breaches” (>200 participants)
2. Collaboration with the European Commission: June 2019 where two Workshops with DPOs and Controllers on personal data breaches took place - 80 participants
3. On 28 November 2019 during the training days organized by Paymaster's Office or PMO training on general data protection rules and principles and personal data breaches 320 participants
4. On 10 January 2019 at DG-Personnel of the EP, a 2-hour training on the EUDPR, with a quiz and a brief case study on Novak case, with a 15 mins intervention of the EDPS Director: 30 participants and other via videoconference
5. On 17&18 January 2019, presentation at ERA on the obligations of the EUDPR, remedies, liability and penalties in case of non-compliance: 70 participants
6. On 23 January 2019, a 2 hour training on the EUDPR at the EUSA with 70 participants
7. On 23 January 2019 a presentation to 12 Chinese students on data protection, the EDPS and algorithms and micro targeting
8. On 6 February 2019, a presentation to 30 lawyers from the association of Tours on data protection, the EDPS and algorithms and micro targeting
9. On 4 February 2019, a half a day training at EUROPOL on the EUDPR, consent, data minimisation, personal breaches scenarios and 2 case studies on access requests
10. On 21 February 2019, a 2 hour training at the EUSA on the EUDPR with 50 participants

11. On 11 March 2019, a 2 hour presentation to DPC's from DG-MOVE and ENER and DPO's from Executive Agencies on joint controllership on research projects
12. On 20 March 2019, a 2-hour training on the EUDPR at the EUSA to 30 participants stressing the revised data protection clauses negotiated between the EDPS and DG-Budget and the substance and form of a joint arrangement
13. On 22 March 2019, a presentation at the OIB on the importance of accountability and data minimisation to 40 staff
14. On 1 April 2019, half a day training to DG TAXUD on joint controllership, restrictions and international transfers
15. On 11 April 2019, presentation on the legal framework, rules, principles and rights to 32 French prosecutors and judges
16. On 19 April 2019, presentation on a Panel in Privacy Days Slovenia on the right to be forgotten to 100 participants mostly DPOs
17. On 20 May 2019, presentation on CCTV at the security services of the ECB and other staff in total 30 participants.
18. On 14 May 2019, a 2-hour training on procurement, joint controllers and processors with a case study at DG-FISMA, EP,60 participants
19. On 24 May 2019, to DG-HR Knowledge Sharing Cafe, presentation on the EUDPR (controllership, content of arrangement, procurement, events organisation, fines : 20 staff with the DPC team and a member of the DPO's team
20. On 14 June 2019, to Internal auditors of EU agencies and joint undertakings on EDPS
21. On 25 June 2019, S&E presentation to 50 EIPA participants
22. On 26 June 2019, the EDPS talked to top management of DG IPOL and DG EXPO (EP) – 25 participants
23. On 28 June 2019, Data protection legal framework: rules, principles and rights to 25 law students from Tyrol, South Tyrol and Trentino
24. On 3 July 2019, Training on the new regulation to EUSA – 30 Participants
25. On 12 September 2019, training on the EDPS role as a supervisory body and policy advisor for the EU institutions and lawmakers to 20 Law students from Hungary
26. On 25 September 2019, presentation on the obligations of the controllers under the new Regulation in EUSA – 30 participants
27. On 3 October 2019, presentation of the EDPS to the top management and middle management of DG DEVCO (EC)
28. On 18 October 2019, presentation to EUSA on EDPS , Erasmus programme participants
29. On 24 October 2019, presentation to EUSA on event management, 60 participants
30. On 5 November 2019, presentation of Data protection legal framework: rules, principles, rights and case law to European Judicial Training network, 32 participants
31. On 8 November 2019, Study visit form students of the Hague University
32. On 8 November 2019, Training on the role of the EDPS and its relationship with the EUI DPOs , 50 participants (Portuguese DPOs)
33. On 22 November 2019, Case studies on procurement , DG DIGIT (EC)
34. On 18 December 2019, Training at EUSA on training on Controllers, processors, joint controllership, 60 participants

2020

1. 45thDPO meeting, of 17th May 2020 in Frankfurt, Case studies on personal data breaches
2. Infographics Video on Personal Data Breaches
3. EUSA Online Talk Case Studies of Personal Data Breaches (>160 participants) recorded video available online.
4. On 23 January 2020, at ESMA a 4-hour training with case studies on the obligations and rights of the EUDPR: 60 participants
5. On 4 February 2020, at EIPA a presentation on the role of the data protection authorities: 50 participants
6. On 18 February 2020, at the EUSA, in Brussels, a 2 hour training on joint controllership: 60 participants
7. On 26 February 2020, at EUSA a 2 hour training on events management: 60 participants
8. On 3 March 2020, at REA a 45 mins presentation to the Director and Top Management (24 managers) and a 2,5 hour training with case studies on the EUDPR to 90 staff
9. On 4 March 2020, at the EUSA in Luxembourg a 2 hour training on joint controllership: 60 participants
10. On 10 March 2020, at EUSA in Brussels a 2 hour training on joint controllership with seven interactive case studies: 70 participants
11. On 4 May 2020, at EMA, a 2,5 virtual training on the role and responsibilities of the controllers, on personal data breaches and on joint controllerships in EMA's processing operations: 322 participants
12. On 2 June 2020 at ERA Valenciennes, a 2 hours virtual presentation on the obligations of the EUDPR, 1h on a case study on events management, 1h on cases studies on breaches and 1h on examples on rights: 65 participants
13. On 23 June 2020 at the Council, a 2 hour virtual presentation on all obligations of the EUDPR with many examples: 50 participants
14. On 1 July 2020, at the EUSA in Brussels, a 2,5 jour training on procurement and outsourcing: 70 participants
15. During most month of August, bilateral trainings were given to 14 newly appointed DPOs and assistant DPOs in over 45 sessions from 60 to 90 minutes each on controllership, video-surveillance, rights, events management, the right to be forgotten, etc
16. On 14 September 2020, at the EUSA Brussels, a 2,5-hour training on procurement and outsourcing: 100 staff
17. On 19, 20, 22 and 23 October 2020, trainings to 200 staff of EUIPO on the EUDPR, transfers, health data in a post-Covid society, safeguards on remote working and teleconferences, case study on physical events, procurement and outsourcing, rights of data subjects, data sharing mechanisms with non EEA international organisations, public authorities and private companies
18. On 18 November 2020, a 2,5 training at the EUSA, Brussels, on data sharing mechanisms with non EEA international organisations, public authorities and private companies: 100 staff
19. On 1 December 2020, presentation on the role of the data protection authorities: 39 participants

20. On 3 December 2020, presentation at the Academy of European Law, Trier on the EUDPR, HR issues, personal file with polls and quiz: 50 participants
21. On 9 December 2020, a 2 hours training on events management at DG-GROW: 39 participants

2021 (until 15 Nov 2021)

1. On 29 January 2021, training on use of social media, transfer of high volume docs in a secured way, choosing DP-friendly ICT tools, use of tools for videoconferences/meetings, controllers-processors' obligations, use of alternative privacy friendly tools/apps in EASME - 160 participants
2. On 21 January 2021, training on Data protection in general and EDPS role in EP trainees at Luxembourg - 100 participants
3. On 3-5 February 2021, presentation on Reinforcing data protection standards in the EU institutions under Regulation 1725 / 2018 , at ERA
4. On 17 March 2021, training on The use of ICT tools and of social media: What are the data protection rules? at EUSA - 100 participants
5. On 25 March 2021, presentation on EUI-owned Social Media Channels to Mitigate Privacy Risks of other Channels at IOCC plenary - 70 participants
6. On 20 April 2021, training on Data Protection and Audit: Principles and Case Studies at DG EMPL (EC) auditors - 12 participants
7. On 29 April 2021, a second training on Data Protection and Audit: Principles and Case Studies at DG EMPL (EC) auditors - 12 participants
8. On 19 April 2021, a training on Data protection in procurement and outsourcing - Safeguarding personal data within contract implementation at Eurojust top and middle management
9. On 20 April 2021, a training on Data protection in procurement and outsourcing - at Eurojust staff
10. On 4 May 2021, training on Data Protection and Audit: Principles and Case Studies at DG EMPL (EC) auditors - 12 participants
11. On 6 May 2021, another round of the training on Data Protection and Audit: Principles and Case Studies at DG EMPL (EC) auditors - 12 participants
12. On 5,12 and 19 May, a DPO training at FRA - 2 participants
13. On 2 and 18 June, another DPO training at FRA - 2 participants
14. On 8 June 2021, a training with title "EUDPR: Is it so complicated to apply in my daily tasks? No!" at EESC - 25 participants
15. On 15 June 2021, a presentation on Supervising data protection compliance: The role of the data protection authorities. Examples from EU institution , at EIPA - 50 participants
16. On 22 June 2021, a training on EUDPR: Conditions and Safeguards in International Transfers to Public Bodies , at EUSA - 100 participants
17. On 30 June 2021, a training on Artificial Intelligence and Anonymization, at EIPA - 10 participants
18. On 14 September 2021, a training on EUDPR: Conditions and Safeguards in International Transfers to private entities , at EUSA - 100 participants
19. On 21 September 2021, a presentation on international transfers, at ECA and CJEU - 100 participants
20. On 12 October, a training on How to apply EUDPR in your daily tasks, at DG FISMA (EC) - 70 participants

21. On 17 November 2021, a training on Artificial Intelligence and Anonymization, at EIPA - 10 participants

CLUSTER 2: LEGISLATIVE CONSULTATION

8) Please provide statistics on Article 42 consultations received and answered for 2018, 2019, 2020, 2021, distinguishing between informal and formal replies (for the latter between comments and full opinions as well).

The EDPS serves as an advisor to the EU legislator on data protection issues. The EUDPR has strengthened the consultative role of the EDPS, both in line with the GDPR and taking into account the practices developed over the past 10 years on the basis of Article 28(2) of Regulation 45/2001.

The EDPS provides guidance on proposed legislation to the European Commission, as the institution with the right to initiate legislation , and the European Parliament and the Council, as co-legislators. Our guidance may take the be given in the following format.

- **Opinions:** our Opinions are issued in response to mandatory requests by the Commission which is legally obliged to seek our guidance on any legislative proposal, or draft implementing acts, 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) 2018/1725[6].

- **Formal Comments:** similar to our Opinions, our Formal Comments are issued in response to a request from the Commission 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. Our Formal Comments are published on our website.

- **Informal Comments:** the European Commission is encouraged to consult the EDPS informally before adopting a proposal that has an impact on data protection. This allows us to provide the Commission with input at an early stage of the legislative process, 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 Commission may also consult the EDPB. In such cases, the EDPS and EDPB work together to issue a joint opinion[7].

[6] 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.

[7] See also Article 20 of the EDPS Rules of Procedure.

The statistics provided below clearly demonstrate that the number of requests for legislative consultation has significantly increased over time. In 2019, the EDPS answered a total number of 35 requests for legislative consultation, whereas in 2020 the number of answers to legislative consultations increased to a total number of 50. By 15 November 2021however, the EDPS had already received a total number of 121 requests for legislative consultation. This steep increase in consultations is attributable to a variety factors.

1) An increasing number of legislative initiatives containing provisions that have an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.

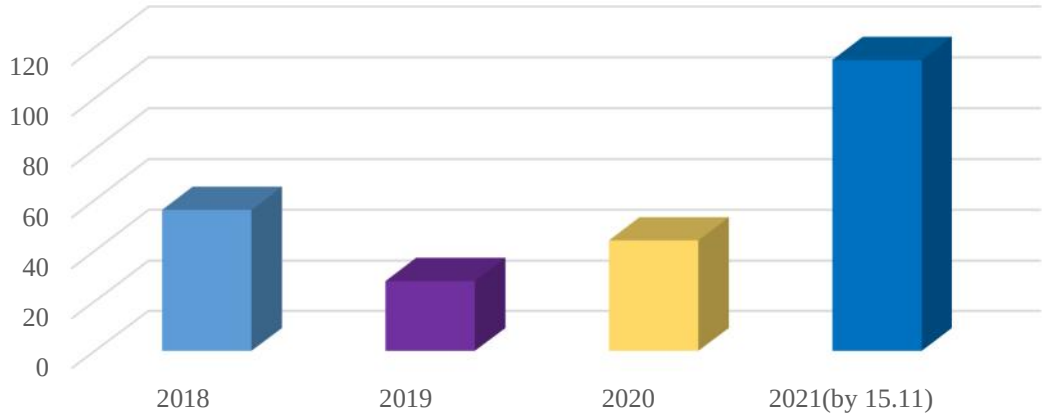
2) The fact that Article 42 of the EUDPR has strengthened the consultative role of the EDPS by establishing a clear and positive obligation for the Commission to consult the EDPS following the adoption of proposals for a legislative act, of recommendations and of proposals to the Council pursuant to Article 218 TFEU (i.e. international agreements) or when preparing delegated acts or implementing acts with "an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data".

3) There is a growing awareness of data protection issues among the Commission's departments. There is also increased awareness of the situations in which consultation of the EDPS is mandatory, as well as the possibility to consult the EDPS informally according to recital (60) EUDPR. This growing awareness is due to the outreach undertaken by the EDPS (in particular through the annual meeting with the Commission services to discuss the annual Commission Work Programme), as well as the important and useful clarifications provided by the Commission in its internal manuals of procedure and the instructions of the Secretary-General regarding the consultation of the EDPS and EDPB.

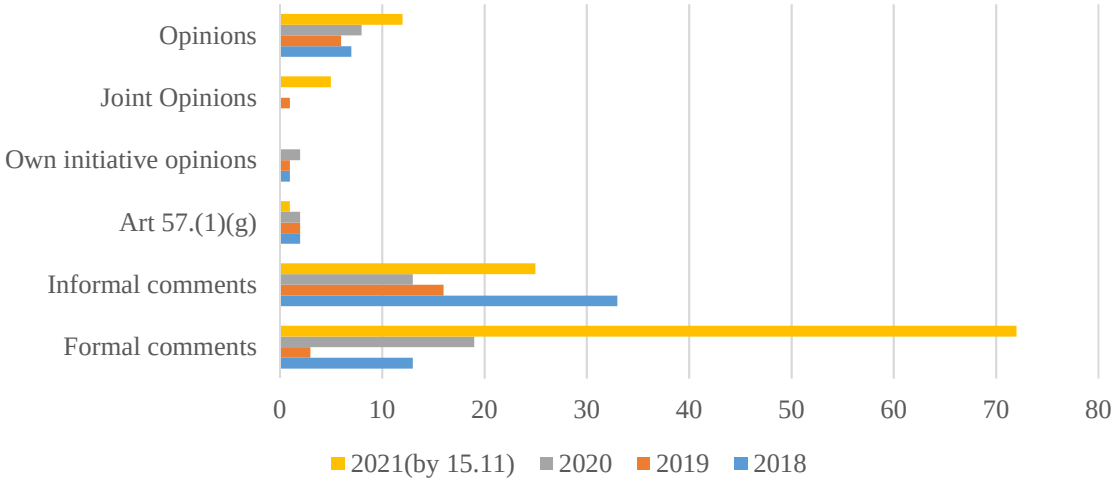
	2018[8]	**2019**	**2020**	**2021 (by 15.11)**
Formal comments	13	3	19	72
Informal comments	33	16	13	25
Joint EDPS-EDPB Opinions	0	1	0	5
EDPS Opinions	7	6	8	12
EDPS own-initiative Opinions	1	1	2	0
Art. 57(1)(g)	2	2	2	1
Total	**56**	**29**	**44**	**115**

[8] Until 12 November 2018, Article 28(2) and 41 of Regulation 45/2001 was still in force. As a result, guidance provided in relation to implementing and delegated acts were provided as informal comments (rather than Opinions), which contributed to the relatively high number of informal comments issued in 2018.

EDPS replies to Legislative Consultations



Type of Consultations issued by EDPS



Beyond these mandatory legislative consultations, the EDPS also has the power to issue Opinions on any issue of relevance to the protection of personal data, addressed to the EU legislator or to the general public, in response to a consultation by another EUI, or on his own initiative[9].

Finally, it should be noted that the Commission occasionally requests advice from the EDPS in relation to implementing acts beyond the context of formal consultations under Article 42(1) or informal consultations on the basis of recital (60) EUDPR. Such requests are typically answered on the basis of Article 57(1)g EUDPR, as indicated in the table above.

[9] Article 58(3) (c) of Regulation (EU) 2018/1725

CLUSTER 3: COOPERATION

9) Please provide feedback on cooperation with other supervisory authorities under Article 61 EUDPR:

a) Please provide statistics for 2018, 2019, 2020, 2021.

The EDPS also cooperates with other DPAs beyond Article 61 of the EUDPR, for instance in the context of its supervisory tasks as provided for sectorial legislation (in particular in the area of Justice and Home Affairs).

Cooperation under Article 61 takes place primarily in an informal way, which contributes to its effectiveness and rapidity. As such, no quantitative indicators are available and in any event they would not necessarily be representative of the useful cooperation under Article 61. See reply under (b) below.

b) What forms did cooperation take – referral of complaints to the competent DPA, what else? Please provide an overview of common cooperation activities.

Article 61 of the EUDPR provides that the EDPS shall cooperate with national supervisory authorities and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA to the extent that is necessary for the performance of their respective duties, in particular by providing each other with relevant information, asking each other to exercise their powers and responding to each other's requests.

Article 26 of EDPS' Rules of Procedure on Cooperation with national supervisory authorities gives effect to Article 61[10].

[10] *"The EDPS shall cooperate with national supervisory authorities and with the joint supervisory authority established under Article 25 of Council Decision 2009/917/JHA(10) with a view to, in particular:*

(a) exchanging all relevant information, including best practices, as well as information in relation to requests to exercise monitoring, investigative and enforcement powers by competent national supervisory authorities;

(b) developing and maintaining contact with relevant members and staff of the national supervisory authorities.

2. Where relevant, the EDPS shall engage in mutual assistance and take part in joint operations with national supervisory authorities, each acting within the scope of their respective competences as set out in the Regulation, the GDPR and other relevant acts of Union law.

3. The EDPS may take part upon invitation in an investigation by a supervisory authority or invite a supervisory authority to take part in an investigation in accordance with the legal and procedural rules applicable to the inviting party"

https://edps.europa.eu/sites/default/files/publication/20-06-26_edps_rules_of_procedure_en.pdf.

Article 6 of the EDPS Rules of Procedure also confirms that the EDPS shall promote cooperation among data protection supervisory authorities as well as with any other public authority whose activities may have an impact on privacy and personal data protection.

As personal data moves from EUIs to public bodies or private entities within the European Economic Area (EEA), the EDPS and national DPAs need to cooperate to ensure effective and complete protection of individuals.

Cooperation with national supervisory authorities is also of crucial importance to enable the EDPS to supervise EUIs effectively. The exchange of relevant information is ongoing with national DPAs, including on important investigations, such as the one about the data protection implications of EUIs' use of Microsoft products and services. For example, EUIs increasingly have recourse to entities subject to the GDPR when outsourcing certain processing activities. Similarly, a need for effective cooperation may arise where an EUI provides and manages an information system for the cooperation of public authorities in EU Member States, or where EUIs process personal data using similar services provided throughout the EEA by a global service provider. It is therefore of paramount importance that efficient and effective cooperation between national DPAs and the EDPS takes place for the EDPS to be able to investigate and assess compliance of EUIs.

- In 2019-2020, the EDPS cooperated with a number of DPAs during the course of one own-initiative inquiry to exchange experiences, information and findings in respective cases.

- In 2020-2021, the EDPS exchanged information with other DPAs about the ongoing investigations on the use of 'Clearview AI' by law enforcement authorities and by Europol.

- In 2020-2021, the EDPS cooperated with a group of DPAs in the context of the EDPB 'TikTok Taskforce', where he exchanged information on the basis of Article 61 GDPR and Article 61 EUDPR on how personal data is processed through the TikTok platform and on the compliance issues being considered by the participating authorities. The EDPS participated in the EDPB TikTok Taksforce in view of a possible further investigation by the EDPS into the use and promotion of the TikTok platform by EUIs and guidance on EUIs' use of social media.

- The EDPS will also be an active participant in the 2022 EDPB coordinated action, that will be carried out according to the EDPB Coordinated Enforcement Framework, by cooperating with participating DPAs in accordance with Article 61 EUDPR and Article 26 of EDPS' Rules of Procedure.

Cooperation with national DPAs is also paramount for the supervision of EUIs, such as Europol, Eurojust, EPPO or Frontex, which collect personal data from national authorities. The efficient supervision of these EUIs sometimes involves coordinated action, the EDPS and the competent supervisory authorities acting each within their scope of competence. For example, in 2020, in the context of the supervision of the processing of data concerning minors by Europol, the EDPS asked national supervisory authorities to perform checks at national level to ensure that the data provided to Europol complied with the applicable legal framework. In that context, the EDPS and DPAs exchanged the necessary information to perform those checks.

The EDPS expects that the need for cooperation with national supervisory authorities is likely to increase over time. Some factors that will contribute to the likely need for increased bilateral and multilateral cooperation are:

- the growing tasks attributed to EUIs in carrying out EU policies;
- the expansion of the EDPS' supervision powers over EUIs that collect the personal data they process from national authorities (Europol, Eurojust, EPPO, Frontex);
- the evolution of technology;
- the policy of building a more autonomous industrial capacity and autonomous provisions of services in the EEA internal market in line with EU law.

These developments will require increased access to cooperation tools for effective, efficient and secure communication, e.g. in the context of handling individual complaints and/or carrying out investigations. In order to do so, the EDPS should be given access to all the tools that facilitate, in a practical way, the exercise of the cooperation.

While the EDPS, as member of the EDPB, has access to the Internal Market Information (IMI) system[11], it currently does not have access to all its functionalities that are necessary to support the efficient and secure exchange of information with DPAs concerning specific cases.

The limitations on the EDPS' access to the IMI system are due, in part, to an interpretation given to the wording of certain provisions of Chapter VII of the GDPR, which refer to "supervisory authorities" as defined by Article 4(21) GDPR[12]. These provisions are also referred to in the Annexes to Regulation (EU) No 1024/2012[13], as well as the Commission's Implementing Decision (EU) 2018/743 on a pilot project to implement the administrative cooperation provisions set out in the GDPR[14]. It is worth noting, however, that each of these instruments were adopted prior to the adoption of the EUDPR.

[11] The Internal Market Information system (IMI) serves as the "internal information and communication system" referred to Article 17 of the EDPB Rules of Procedure.

[12] Article 4(2) GDPR defines a 'supervisory authority' as an independent public authority which *is established by a Member State* pursuant to Article 51 GDPR.

[13] See point 11 of Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation'), referring to Article 56, Articles 60 to 66 and Article 70(1) GDPR.

[14] Commission Implementing Decision (EU) 2018/743 of 16 May 2018 on a pilot project to implement the administrative cooperation provisions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council by means of the Internal Market Information System, 0.J. 18.5.2018, L 123-115.

Examples of instances in which greater access to IMI functionalities would be useful include functionalities to initiate or respond to requests for mutual assistance or joint operations. Such a need arises not only in the context of own-initiative investigations as described above, but also in the context of handling complaints. Currently, the EDPS rarely forwards or directly receives complaints to and from DPAs. This occurs, for example, in cases concerning sensitive data with significant impact on the rights and freedoms, health or life of an individual, or where a large number of individuals are involved[15]. For example, over the years, most recently in 2020, the EDPS received a number of complaints concerning European Schools, where we cooperated with a national supervisory authority to clarify that it is in fact their responsibility to supervise European Schools' compliance with the GDPR.

In 2018 and 2019, the EDPS also investigated a number of complaints referred by a national DPA concerning the processing of personal data by the Commission in the context of public consultations using the 'EU Survey' tool. The national DPA was the interlocutor with the complainants. For the exchange of relevant information concerning such complaints, it would also be more practical to be able to use the full array of IMI procedures and workflows to facilitate the efficient and effective exchange of relevant information.

Moreover, the EDPS does not systematically receive updates from national supervisory authorities concerning ongoing cross-border cases. Irrespective of whether an Article 65 GDPR procedure is initiated at a later stage in a particular case, receiving such information may also be relevant for the EDPS in the performance of his duties. In particular, the information shared by a Lead Supervisory Authority concerning a controller or processor providing services that are also used by EUIs may be relevant in the context of the EDPS' supervision and enforcement activities. In the same vein, the EDPS might have an interest in obtaining an opinion of the EDPB pursuant to Article 64(2) GDPR on a matter of general application of the GDPR relevant to a case it is investigating.

The EDPS considers that Article 61 EUDPR provides a sufficient legal basis to enable efficient cooperation with national supervisory authorities. To be truly effective and efficient however, operational access to all relevant functionalities of the IMI system is needed[16]. The EDPS considers that a combined reading of Article 61 of the EUDPR, read in light of recitals (4) and (5), and of the GDPR provides a sufficient legal basis to extend access to all relevant functionalities of the IMI system, including the procedures regarding mutual assistance and joint operations. Further intervention by the Commission or the EU legislator is only likely to be necessary if obstacles to the efficient exchange of information persist over time.

[15] In all cases, however, the EDPS will refer complainants to the relevant DPA or another competent authority.

[16] Having one system to exchange information between national supervisory authorities and another channel to exchange the same information on the same cases between EDPS and national DPAs is not very efficient for either the EDPS or the national supervisory authorities concerned.

The EDPS considers that Article 61 EUDPR provides a sufficient legal basis to enable efficient cooperation with DPAs. To be truly effective and efficient, however, operational access to all relevant functionalities of the IMI system is needed[17]. Further intervention by the Commission or Union legislator is only likely to be necessary if obstacles to the efficient exchange of information persist over time.

10) Article 62 EUDPR created a horizontal framework for supervision coordination to which more and more large-scale IT systems will be moved in the future. Do you consider that it has led / will lead to increased efficiency of resource use?

The EDPS currently serves as the Secretariat of the Supervision Coordination Groups ('SCGs') of the Schengen Information System, the VISA Information system, the Eurodac Information System, the Customs Information System and of the Europol Cooperation Board. The legal basis for this vertical – system-related – coordination of supervision is contained in the respective legal acts establishing the IT-systems.

According to Article 62(2) EUDPR, the EDPS and the national DPAs shall exchange relevant information, assist each other in carrying out audits and inspections, examine the difficulties of interpretation or application of that Regulation and other applicable EU acts, study problems with the exercise of independent supervision or with the exercise of the rights of individuals , draw up harmonised proposals for solutions to any problems and promote awareness of data protection rights. In particular, Article 62(3) EUDPR provides that, for the purposes laid out in Article 62(2) EUDPR, the EDPS and the national supervisory authorities shall meet at least twice a year **within the framework of the EDPB**. The move of the Secretariat role of the Supervision Coordination Groups from the EDPS to the EDPB is expected to happen in the next year.

The EDPS believes that the current Supervision Coordination Groups model does not allow for horizontal and efficient discussions on issues concerning more than one IT system, such as when interoperability between such systems is at stake. The move of the Secretariat role of the Supervision Coordination Groups from the EDPS to the EDPB will not only lead to an efficient use of resources, but will also increase the coordination between the EU's DPAs within the Coordinated Supervision Committee (CSC) and the EDPB itself, as the latter will serve as a unique point of contact and will possibly reduce any discussions and work overlap.

Article 62 also creates a horizontal framework for the supervision coordination of EUIs that will also be taken over by the EDPB within the CSC. Currently, the CSC is dedicating meetings to the supervision of EPPO and Eurojust. It will also deal with the supervision of Europol, once the Europol Cooperation Board is transferred to the EDPB. It is likely that the coordinated supervision mechanism put in place by Article

[17] Having one system to exchange information between national supervisory authorities and another channel to exchange the same information on the same cases between EDPS and national DPAs is not very efficient for either the EDPS or the national supervisory authorities concerned.

62 will -also be used for the supervision of Frontex as the ECBG Regulation establishes a shared responsibility between the Agency and national authorities responsible for border management for the implementation of the European integrated border management. This requires in particular that the Agency and the host EU Member State determine their responsibilities in terms of data protection (Article 88 ECBG Regulation). The expansion of the mandates of the Justice and Home Affairs Agencies and bodies (JHA agencies and bodies), together with the increase in data exchanges between them as well as with national authorities, will require closer cooperation between the EDPS and SAs under the umbrella of the CSC. The former experience of cooperation within the Europol Cooperation Board since May 2017 has shown that the EDPS and SAs need adequate tools to be able to exchange information that is classified in order to be able to deliver opinions, conduct joint inspections, or investigate complaints. Additional obstacles could stem from national provisions, which for instance do not allow for the EDPS to participate in national inspections even if an EUI is making use or has access to a national information system.

11) Article 68(6) GDPR restricts voting rights of the EDPS in Article 65 GDPR procedures to those that concern principles and rules that correspond in substance to those applicable to the Union institutions, bodies, offices and agencies. When participating in these procedures, how do you assess whether this is the case? Based on which horizontal criteria?

Article 68(6) provides that "*in the cases referred to in Article 65, the EDPS shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation*".

When interpreting Article 68(6) GDPR, the EDPS primarily takes into account the wording of the GDPR itself, the wording of the EUDPR, as well as the legislative history that preceded the adoption of both instruments.

Article 2(3) GDPR provides that "*[f]or the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98*"[18].

Recitals (4) and (5) of the EUDPR reiterate the overall intention of the Union legislator to provide for a "*strong and coherent data protection framework in the Union (...) to allow its application in parallel with Regulation (EU) 2016/679*".

"*It is in the interest of a coherent approach to personal data protection throughout the Union, and of the free movement of personal data within the Union, to align as far as*

[18] Article 98 GDPR additionally specifies that "*[t]he Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data*".

possible the data protection rules for Union institutions, bodies, offices and agencies with the data protection rules adopted for the public sector in the Member States. Whenever the provisions of this Regulation follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the CJEU, be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679".

The aforementioned provisions and recitals make it clear that the "principles and rules" contained in the GDPR and the EUDPR have been aligned as much as possible. It also confirms the need for commonality in the interpretation of the respective provisions. While the EUDPR contains provisions adapted to the EUIs' specificities , both the wording and legislative history of the GDPR and EUDPR confirm the intention of the EU legislator to ensure as much consistency as possible.

The EUDPR did not yet exist at the time of drafting the GDPR. As a result, the EU legislator could not fully anticipate the extent to which provisions of both instruments would be aligned when drafting Article 68(6) GDPR. With the final text of the EUDPR now at hand, it is clear that the EU legislator succeeded in the objective of achieving a very high degree of homogeneity and commonality (i.e. "correspond in substance") between both instruments.

At the same time, it is clear that the GDPR in general, and Article 65 GDPR in particular, contain or (indirectly) refer to provisions for which there is no substantially equivalent provision in the EUDPR *per se*. For example, the EUDPR does not contain any provision to identify the 'main establishment' or 'lead supervisory authority'. The EUDPR also does not contain, for instance, any provision allowing the EDPS to approve 'binding corporate rules'. As the EDPS is not competent to approve such binding corporate rules, it is also not subject to the obligation contained in Article 64(1)(f) of the GDPR, which requires the competent supervisory authority to seek an Opinion of the EDPB when it aims to approve binding corporate rules.

It is against this background that the EDPS interprets Article 68(6) GDPR.

Article 65 of the GDPR requires the EDPB to issue a binding decision:

(a) to resolve disputes concerning a "relevant and reasoned objection";

(b) whenthere are conflicting views on which of the supervisory authorities concerned is competent for the "main establishment";

(c) where a competent supervisory authority does not request the opinion of the EDPB in the cases referred to in Article 64(1), or does not follow the opinion of the EDPB issued under Article 64.

Decisions of the EDPB under Article 65(1)(a) GDPR by definition concern the issue of whether there is an infringement of the GDPR or whether envisaged action in relation to the controller or processor complies with the GDPR[19]. As there is a very high degree of commonality between the provisions of the GDPR and EUDPR,

[19] See Article 4(24) GDPR.

decisions of the EDPB under Article 65(1)(a) shall very often concern principles and rules applicable to the EUIs.

Because Article 68(6) GDPR refers to principles and rules applicable to EUIs, it is not required that the specific case that the EDPB is called to decide upon involves an EUI. Instead, what matters is whether the decision of the EDPB shall be relevant to the interpretation of the EUDPR because it concerns principles and rules that have a substantial "counterpart" in the EUDPR. As there are relatively few instances where the EUDPR does not contains rules and principles that correspond in substance to the rules and principles contained in the GDPR (or vice versa), the EDPS will only seldom not have voting rights in the EDPB's decisions under Article 65(1)(a) GDPR. Although a careful case-by-case assessment remains necessary).

The situation may prove to be different regarding Article 65(1)(b), as the EUDPR does not contain any provision to identify the 'main establishment'. While it cannot be excluded that such decisions also give rise to matters of interpretation that concern principles and rules that correspond in substance to principles and rules contained in the EUDPR (e.g., the concept of "controller"), the EDPB might also be called upon to issue decisions under Article 65(1)(b) GDPR where this is not the case. Similar considerations also apply in relation to Article 65(1)(c) GDPR, which might, for example, concern the extent which a supervisory authority has followed an Opinion of the EDPB that concern the approval of binding corporate rules.

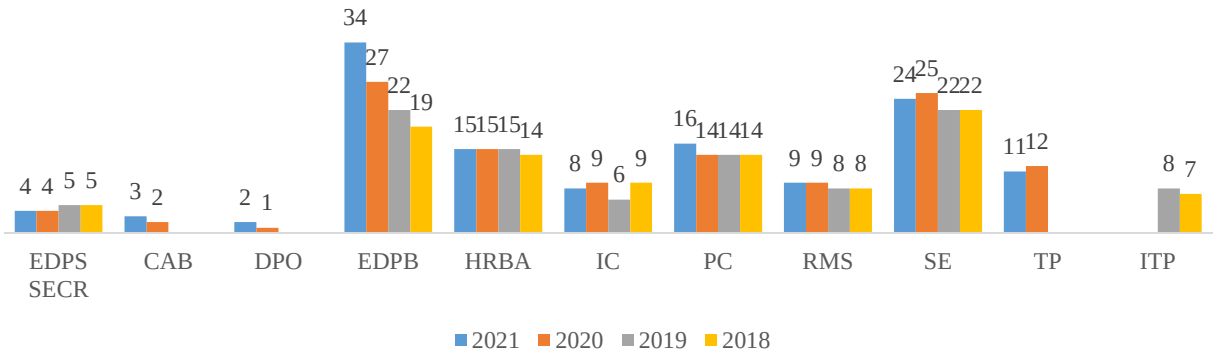
In light of the above, the EDPS carefully assesses decisions and the substantive issues raised on a case-by-case basis in order to assess its voting rights pursuant to Article 68(6) GDPR. To date, the EDPS has exercised its voting right in relation to each EDPB decision under Article 65(1)a GDPR[20], as each of these decisions has concerned principles and rules applicable to the EUIs which correspond in substance to those of the GDPR. To date, the EDPB has not yet been called upon to issue decisions under Article 65(1)(b) GDPR or Article 65(1)(c) GDPR, so the EDPS is currently not in a position to provide additional information concerning the EDPS' voting rights in relation to these EDPB decisions.

[20] At the moment of writing, the EDPB has issued two decisions under Article 65(1)(a) GDPR, namely Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR (adopted on 9 November 2020) and Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR (adopted on 28 July 2021).

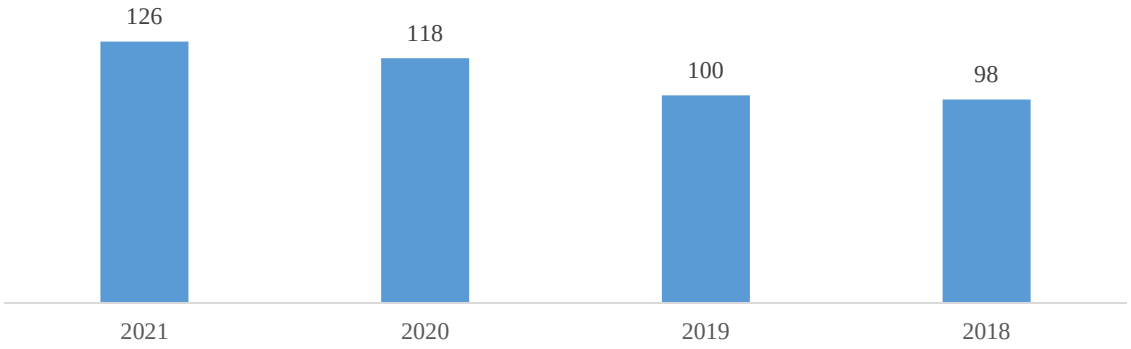
CLUSTER 4: RESOURCES

12) Please provide staff figures (full-time equivalents) for 2018, 2019, 2020, 2021 and the forecast for 2022 (incl. a breakdown per area of tasks/activities).

Staff figures broken down per unit/sector*

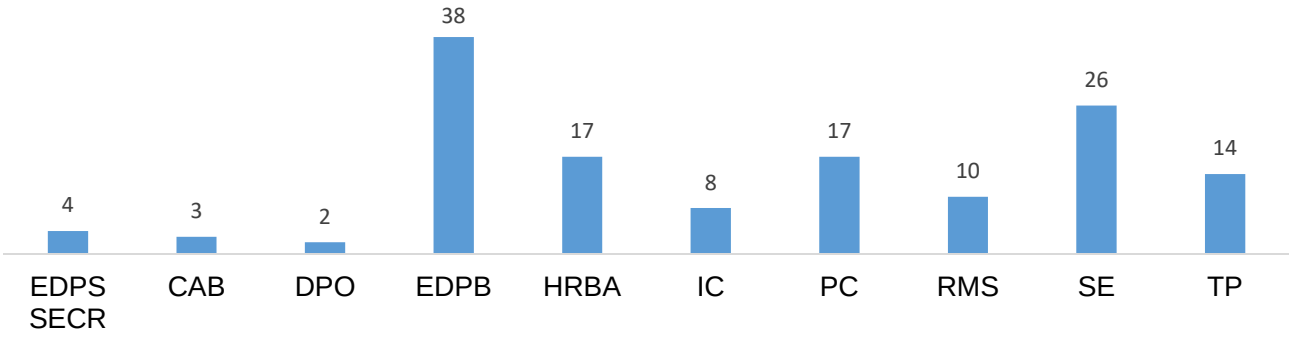


Overall staff figures*



* Reference dates: 16/11/2021, 31/12/2020, 31/12/2019, 31/12/20218

Forecast of staff distribution for 2022**



** Includes staff active on 01/01/2022 and new posts for 2022

13) Please provide the figures of EDPS budget for 2018, 2019, 2020, 2021 and the forecast for 2022

2018 (executed)	2019 (executed)	2020	2021	DB2022
€ 13.118.368	€ 15.155.802	€ 14.195.886	€ 19.463.193	€ 20.202.000

14) How would you assess the EDPS' resources from a human, financial and technical point of view?

The EDPS would need more resources (mostly human) to cope with the high workload resulting from all the new tasks entrusted to both entities by the legislators.

These new tasks and the creation of the EDPB,, occurred during the years where austerity policies were required by the EU Member States and therefore, we were not able to request all t necessary staff.

The EDPS is trying to compensate by asking for gradual and steady growths every year until the size of the staff and the budget reach a level that matches its level of responsibilities.

In view of the acceleration of digital transformation, and the resulting digitalisation, the EDPS would need more human resources with a technical background, in particular an IT background, as the majority of the EDPS' staff have a legal background. Also, special expertise such as in the field of artificial intelligence (AI), and data analysis will be needed in the future

In particular, Article 63(6) of the Commission's proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)[21] states that the EDPS "shall act as a market surveillance authority" for EUIS that fall within the scope of the Proposal. While the EDPS welcome this designation of the EDPS as the competent authority and the market surveillance authority for AI, the fulfilment of the new duties foreseen for the EDPS, acting as notified body, would require significantly higher financial and human resources than what is currently envisaged.

The digital transformation of EUIs' internal and external communication, as well as other core business activities, have led to the outsourcing of numerous activities with increased reliance on Information and Communication Technology providers. The complexity of these contracts, the implementation of the Schrems II strategy in the long run, the new tasks deriving from the EUDPR as well as the shift from administrative to core business activities require more staff in order to ensure faster, more effective and strategic handling of cases.

[21] COM (2021) 206 final.

Lastly, in view of the expansion of the mandates of EUIs active in the field of the Area of Freedom, Security and Justice (Europol, Eurojust, Frontex, European Asylum Office) and the start of operations of European Public Prosecutors Office (EPPO), the EDPS will have to dedicate more resources to the supervision of this area, which is particularly sensitive in terms of impact on individuals' fundamental rights.

A high proportion of EDPS activities are reactive, in response to EUIs, individuals and other stakeholders. 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 the EUDPR). 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 the planning and executing of other, proactive, activities, so far as possible within these constraints.

As the statistics provided under question 8 clearly illustrate, there also has been a considerable increase in the number of requests for Joint Opinions in 2021. As the EDPS authors Joint Opinions together with the EDPB, such files require additional cooperation and coordination.

While the Unit within the EDPS in charge of legislative consultation has grown slightly since 2018, its increase in staff is not commensurate with the overall increase of the 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.

The work of the EDPB and its expert subgroups has increased and intensified. As the work involved concrete cases or general principles and matters that are of particular relevance for the processing of personal data by EUIs, the participation of different units in the meetings and input in the work of the expert subgroups have substantially increased. In 2020, the number of meetings of the EDPB expert subgroups where the EDPS' involvement was deemed necessary had doubled or tripled (depending on the subgroup) compared to 2019. Two new taskforces were created in 2020 that require significant involvement. The trend of increasing EDPB-related work is expected to continue in 2021 and in the next years.

In order to ensure appropriate alignment of the enforcement of both the GDPR and the EUDPR, the EDPS will therefore need to have sufficient resources available to ensure the follow-up of the increasingly relevant work of the EDPB, in particular for cooperation and enforcement actions within EDPB (e.g. in the context of EDPB Coordinated Enforcement Framework and Support Pool of Experts) and with national DPAs (e.g. for joint operations).

Finally, there is a specific resource issue in relation to the Supervisor. Indeed, the elimination of the Assistant Supervisor has inevitably determined an increase in the workload of the Supervisor as the EDPS has become a monocratic body.

15) More specifically, is the EDPS equipped to contribute to the EDPB's activities in line with its mandate? How many persons (FTE) contribute to the EDPB's activities (please break down by specific activities of the EDPB)

As the EDPS provides the Secretariat of the EDPB, it should first be clarified that the reply to this question does not relate to the Secretariat of the EDPB but to the EDPS' involvement within the EDPB.

Under the GDPR, the EDPS is not only tasked with providing the secretariat for the EDPB[22], but is also a full member of the EDPB.

The success of the EDPB requires a strong EDPB Secretariat, but is equally dependent on the capacity of all its members, including the EDPS, to fully engage in the activities of the Board so as to deliver high quality results. In this capacity, the EDPS actively contributes to the activities of 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. In this context, the EDPS often plays a leading role as a lead rapporteur, co-rapporteur, or otherwise actively contributes to the work of the EDPB. The EDPS also serves as Chair of the EDPB expert subgroup on key provisions.

The active contribution of the EDPS to the EDPB's activities is also necessary to ensure consistency in the interpretation of the EUDPR and GDPR. As indicated previously, the Union legislator has sought to ensure as much alignment as possible between the respective provisions of the EUDPR and GDPR[23]. It is by actively contributing to the EPDB's activities that homogenous interpretation can be achieved in practice.

As far as legislative consultations are concerned, Article 42(2) EUDPR provides for the possibility for the Commission to consult the EDPB and the EDPS together in case of acts of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data[24].

It is very difficult to precisely quantify the various contributions made by the EDPS to the EDPB, as these contributions take many forms (e.g. as lead or co-rapporteur, in the form of written comments, oral interventions etc.). Each of these contributions requires internal coordination (typically across units) and external engagement (both at expert subgroup and plenary level). Notwithstanding the overall increase in workload, the EDPS has, in line with its mandate, played a very active role in some of the most important EDPB files. The following sections provide an overview of the EDPB files for which the EDPS made a substantial contribution in 2019, 2020 and 2021.

[22] Article 75(1) GDPR. In accordance with Article 75(3) GDPR, the staff of the EDPS involved in carrying out the tasks conferred on the Board are subject to separate reporting lines. In accordance with Article 75(4) GDPR the terms of the cooperation between the EDPS and the EDPB have been laid down in a Memorandum of Understanding, available at https://edpb.europa.eu/sites/default/files/files/file1/memorandum_of_understanding_signed_en.pdf .

[23] See also the reply to question 11 above.

[24] See also the reply to question 8 above

EDPB files in which the EDPS made a substantial contribution in 2019

- EU - U.S. Privacy Shield - Second Annual Joint Review report;
- EU - U.S. Privacy Shield - Third Annual Joint Review report;
- Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) Art. 64 GDPR Opinion on the draft administrative arrangement by ESMA;
- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects;
- Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725);
- EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI);
- Statement 3/2019 on an ePrivacy regulation;
- Statement 2/2019 on the use of personal data in the course of political campaigns;
- Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities;
- Opinion 4/2019 on the draft AA between EEA and non-EEA Financial Supervisory Authorities;
- EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection;
- Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA;
- Amendment to the EDPB rules of procedure, in order to formally establish the Coordinated Supervision Committee within the EDPB;
- Guidelines 3/2018 on the territorial scope of the GDPR (after public consultation);
- EDPB contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention);
- EDPB Response to BEREC request for guidance on the revision of its guidelines on net neutrality rules;

EDPB files in which the EDPS made a substantial contribution in 2020

- EDPB cooperation with the European Commission in the context of its initial and in-depth investigation of the proposed Google/Fitbit merger;
- Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679;
- Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems;

- Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications;
- The first binding EDPB decision on the basis of Article 65 of the GDPR, which concerns a draft decision by the Irish DPA on Twitter International Company;
- Guidelines 3/2019 on processing of personal data through video devices;
- The EDPB Strategy 2021-2023, which sets out the EDPB's strategic objectives, grouped around four pillars, as well as three key actions per pillar to help achieve these objectives;
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR;
- Statement on privacy implications of mergers;
- The EDPB contribution to the evaluation and review of the GDPR under Article 97 of the GDPR;
- Guidelines 2/2020 on articles 46(2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies;
- Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak;
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak;
- Letter regarding the Polish presidential elections taking place via postal vote;
- Statement on data subject rights in connection to the state of emergency in Member States and a letter regarding the Hungarian Government's Decree 179/2020;
- Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Article 28(8) GDPR);
- Statement on the data protection impact of the interoperability of contact tracing apps and Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak;
- Publication of a new register containing decisions taken by national DPAs following the One-Stop-Shop cooperation procedure (Article 60 of the GDPR);
- Guidelines 08/2020 on the targeting of social media users;
- Final version of the Guidelines 4/2019 on Article 25 on Data Protection by Design & Default (after public consultation);
- Setting up of a Coordinated Enforcement Framework, which provides a structure for coordinating recurring annual activities by DPAs;
- Establishment of a Support Pool of Experts (SPE) on the basis of a pilot project. The goal is to provide material support to EDPB Members in the form of expertise that is useful for investigations and enforcement activities and to enhance cooperation and solidarity between EDPB Members by sharing, reinforcing and complementing strengths and addressing operational needs;
- Final version of the Guidelines 06/2020 on the interplay of the Second Payment Services Directive (PSD2) and the GDPR.

EDPB files in which the EDPS made a substantial contribution in 2021

- EDPB-EDPS Joint Opinion 1/2021 on standard contractual clauses between controllers and processors;
- EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries;

- Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive;
- EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research;
- Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention);
- EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act);
- Statement 03/2021 on the ePrivacy Regulation;
- EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery;
- Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom;
- Guidelines 03/2021 on the application of Article 65(1)(a) GDPR;
- Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom;
- Statement 05/2021 on the Data Governance Act in light of the legislative developments;
- EDPB Response to Mr. de Serpa Soares, Under-Secretary-General for Legal Affairs and UN Legal Counsel (May 2021);
- EDPB response to Mr Miguel de Serpa Soares regarding the ongoing dialogue between the EDPB and the United Nations on data protection (November 2021);
- Final version of the Recommendations 1/2020 on supplementary measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (after public consultation);
- EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act);
- Opinion 20/2021 on Tobacco Traceability System;
- EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro - to the European Central Bank;
- Guidelines 02/2021 on virtual voice assistants (after public consultation);
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR (after public consultation);
- Guidelines 10/2020 on restrictions under Article 23 GDPR;
- EDPS proposal on 2022 coordinated action of the EDPB in the context of the Coordinated Enforcement Framework;
- Statement on the Digital Services Package and Data Strategy
- Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR;

- Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited;
- Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR.

While reinforcement of the EDPB Secretariat is needed to enable the EDPB to deal with the increased workload, a similar reinforcement of the EDPS' units, engaged in the substantive work of the EDPB, (much like national supervisory data protection authorities)is equally valid and important.

As an example, the EDPS had to prepare for around 5 to 6 plenaries of the Article 29 Working Party – the predecessor of the EDPB - per year until May 2018. As from May 2018, the rhythm of plenaries substantially increased with 11 EDPB plenaries in 2019, 27 in 2020 and 15 in 2021.

In general, it would be highly desirable for the EDPS to be better equipped to contribute to the EDPB's activities. This is because the workload at EDPB expert group level and Plenary level has substantially increased. As a result, it might sometimes be challenging for the EDPS to contribute meaningfully to the EDPB's activities while fulfilling its other tasks at the same time.

Additional messages with regard to Chapter IX, in light of Article 98 EUDPR.

The introduction of a specific Chapter on the processing of operational personal data, in line with the Law Enforcement Directive, in the EUDPR, is welcomed by the EDPS. This provides a baseline applicable to all EUIs that process operational personal data.

Scope of Chapter IX as provided in Article 2(2) EUDPR.

Despite achieving the creation of that baseline, the exclusion of Europol and EPPO, combined with the existence of specific (and almost self-standing) provisions in the Eurojust Regulation and the very recent authorisation given to Frontex to process operational personal data under the new Article 90 of the European Border and Coast Guard Regulation (Reg. 2019/1896), has greatly limited the applicability of the provisions of Chapter IX. De facto, the EDPS has not applied any of these provisions in his consultations, audits, investigations or complaints. The alignment of the Europol Regulation (amendments currently in the final stage of the legislative process) will most likely contribute to change this situation.

The tables hereunder show the number of consultations, audits, investigations and complaints related to the processing of operational data for Europol, Eurojust, EPPO and Frontex for 2019, 2020, 2021.

2019

	Consultations	Prior consultations	Audits	Investigations (inquiries)	Complaints
Europol	9	3	2	4	3

2020

	Consultations	Prior consultations	Audits	Investigations (inquiries)	Complaints
Europol	14	3	0	1	2
Eurojust	5	0	0	0	0
EPPO	5	1	0	0	0
Frontex	0	0	0	0	0

2021

	Consultations	Prior consultations	Audits	Investigations (inquiries)	Complaints
Europol	12	3	1	1	5
Eurojust	3	0	1	0	0
EPPO	1	1	0	0	0
Frontex	0	0	0	0	0

Despite the limited experience in practice, we can already foresee a series of shortcomings, linked to the narrow scope of Article 2(2) EUDPR.

The fragmentation of the provisions on EDPS powers creates confusion as to the role of the EDPS as supervisory authority, as all EUIs are not put on the same footing (despite that being the intention of the legislator when it incorporated a dedicated Chapter on the processing of operational personal data to the EUDPR). It is not clear for instance to what extent the EDPS can conduct audits as such investigative powers are not explicitly mentioned in any of the specific instruments (except for Europol in relation to joint inspections with national experts). It is not clear either if EUIs processing operational data have the same legal obligation to cooperate, on request, with the EDPS, as set out under Article 32 EUDPR.

Other shortcomings stemming from the fragmentation of the legal framework can be detected in other provisions of the EUDPR.

- **The tasks and duties of the DPO** – there is no justification for the DPO to have different tasks and obligations with regard to the processing of administrative data or the processing of operational personal data.

- **Cooperation and coordinated supervision between the EDPS and national DPAs** - The EUDPR does not provide for Article 61 and 62 to apply to the cooperation concerning the processing of operational personal data, despite the fact that (1) such cooperation is particularly relevant in the context of the supervision of EUIs such as Europol, EPPO, Eurojust or Frontex, as these EUIs process data collected from national authorities, and that (2) the Europol

Cooperation Board will be integrated to the Coordinated Supervision Committee once the reform of the Europol regulation is completed.

- Article 31, which provides for the obligation of the data controller to maintain a record of processing activities and to make it available on request to the EDPS, does not apply either to the processing of operational personal data. This provision is however essential to ensure the transparency of data controllers' activities related to the EDPS, a supervisory tool particularly important in this field of activity.

Relation between Chapter IX EUDPR and specific instruments.

Chapter IX replicates in a large part most of the provisions of the Law Enforcement Directive. It therefore integrates into a Regulation provisions drafted in the context of a Directive. The EDPS understands that Chapter IX provides a baseline (as the Law Enforcement Directive does for national law enforcement authorities), which acts as *lex specialis* vis-à-vis the general provisions of the EUDPR. The specific instruments regulating EUIs processing operational personal data (Europol, Eurojust, EPPO, Frontex) should further specify these provisions, where necessary, to adjust them to the particularities of the processing activities of these EUIs(as done at national level by EU Member States when transposing the Law Enforcement Directive).