EUROPEAN
COMMISSION

Brussels, 14.10.2022
COM(2022) 530 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

First report on the application of the Data Protection Regulation for European Union institutions, bodies, offices and agencies (Regulation 2018/1725)

Contents

1 Introduction

The Data Protection Regulation for the European Union institutions, bodies, offices and agencies[1] ('EUDPR') is the main[2] data protection framework for the EU institutions, bodies, offices and agencies ('EUIBs') when they process personal data as controllers or processors. The Regulation forms a pillar of good governance and good administrative conduct at EU level. It has applied since 11 December 2018[3], when it repealed and replaced its predecessor, Regulation (EC) 45/2001[4].

This communication presents the first report on the application of the EUDPR, in line with Article 97 of the Regulation. It also reviews the legal acts adopted on the basis of the Treaties that regulate the processing of operational personal data[5] by EU bodies, offices or agencies when carrying out activities within the scope of police cooperation and judicial cooperation in criminal matters[6], in line with Article 98 of the EUDPR.

The Commission has collected information on the application of the EUDPR through a survey launched in October 2021, where the EUIBs were invited to share their experience in applying the EUDPR. Altogether 56[7] EUIBs replied, and the statistics on EUIBs presented in the report are based on these replies[8]. A separate request for contribution was sent to the European Data Protection Supervisor (EDPS) in its role as a supervisory authority[9]. Lastly, the Commission also published a call for evidence[10], which allowed the public to comment as well. The issues raised in the very few submissions received in reply to the call for evidence are addressed in this report.

This report situates the EUDPR in the framework of EU data protection law, presents its application by the EUIBs and the EDPS's activities, and analyses the application of the chapter applicable to EU bodies and agencies carrying out activities within the scope of police cooperation and judicial cooperation in criminal matters. The report concludes by outlining the way forward.

---

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), OJ L 295, 21.11.2018, p. 39-98, http://data.europa.eu/eli/reg/2018/1725/oj.

[2] Some agencies in the area of justice and home affairs have specific data protection rules in their establishing acts that either complement or apply instead of the EUDPR, see Section 6.

[3] In line with Article 101(2) EUDPR, it has only applied to Eurojust since 12 December 2019.

[4] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22, http://data.europa.eu/eli/reg/2001/45/oj.

[5] Article 3(2) EUDPR.

[6] Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty of the Functioning of the European Union (TFEU).

[7] The survey was sent to the EUIBs that existed at the time (list: http://publications.europa.eu/code/en/en-5000900.htm).

[8] Percentages given in this report are always out of those EUIBs that replied to that specific question in the survey.

[9] European Data Protection Supervisor, Contribution by the European Data Protection Supervisor to the Report on the application of Regulation (EU) 2018/1725, the 'EUDPR', 21 December 2021, https://edps.europa.eu/system/files/2022-04/20-12-21-contribution_edps_report_eudpr_en_0.pdf

[10] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13256-Data-Protection-Regulation-for-EU-institutions-bodies-offices-and-agencies-report-on-application_en.

2 Separate data protection rules for EU institutions, bodies, offices and agencies aligned with EU data protection legislation

The main data protection instruments in the EU are the General Data Protection Regulation ('GDPR')[11], the Law Enforcement Directive ('LED')[12] and the ePrivacy Directive[13]. However, they do not apply to the processing of personal data by EUIBs[14]. Therefore, separate, yet aligned data protection rules for the EUIBs are necessary. The EUDPR provides these rules.

To ensure a consistent approach to protecting personal data and their free movement in the EU, the EUDPR is aligned as far as possible with the data protection rules adopted for the public sector, laid down in the GDPR and the LED. Whenever the EUDPR follows the same principles as the GDPR, it should be interpreted in the same way, as it should be understood as equivalent to the GDPR[15]. The same can be assumed with the rules aligned with the LED.

The EUDPR is adapted to the specific context of the EUIBs as described in the points below.

- As its scope of application is exclusively the EUIBs as public bodies, several provisions from the GDPR that are only relevant for the private sector have been omitted. For example, the possibility to process relying on the legal basis of 'legitimate interests' of the controller does not exist in the EUDPR[16].
- Several empowerments for the Commission to adopt implementing or delegated acts are not repeated as such, but instead the EUDPR refers to the GDPR or the LED. For example, the EUDPR does not contain a mechanism to adopt adequacy decisions for international transfers, but adequacy decisions adopted under the GDPR or the LED can also be relied upon by the EUIBs.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 4.5.2016, p. 1-88, http://data.europa.eu/eli/reg/2016/679/oj.

[12] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131, http://data.europa.eu/eli/dir/2016/680/oj.

[13] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201. 31.7.2002, p. 37-47, https://data.europa.eu/eli/dir/2002/58/oj.

[14] Article 2(3) GDPR, Article 2(3)(b) LED. The ePrivacy Directive as such does not apply, but Article 37 of the EUDPR obliges EUIBs to protect information transmitted to, stored in, related to, processed by and collected from the terminal equipment of users accessing their publicly available websites and mobile applications in accordance with Article 5(3) of Directive 2002/58/EC.

[15] See recital 5 EUDPR.

[16] This mirrors the situation under its predecessor, Regulation (EC) 45/2001, which did not include the 'legitimate interest' ground either. Recital 22, second sentence, of the EUDPR clarifies that 'processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for [their] management and functioning', meaning that such processing operations, e.g. for ensuring physical access control to EUIB premises, are also covered.

- The EUDPR also directly establishes the EDPS, setting out its tasks, powers and appointment procedures. Under the GDPR and the LED, the respective supervisory authorities are established under national law, in line with the requirements of these two acts.
- The EUDPR's chapter applicable to EU bodies and agencies in the criminal law enforcement[17] area is functionally equivalent to the LED for those bodies and agencies. However, as a directly applicable Regulation, it is formulated differently. It provides general rules to be supplemented by specific provisions in the establishing acts of bodies and agencies acting in this area where necessary. It provides a tailored regime for processing operational personal data taking into account the specific nature of this sector, for instance the rules on informing data subjects, which ensure that investigation are protected.

3 Implementation of the EUDPR in EUIBs

3.1 EUIB's role as controllers

The general feedback from EUIBs shows that the first years of applying the EUDPR have successfully contributed to strengthening their general data protection culture. In this regard, 94% of EUIBs stated that the entry into force of the EUDPR increased their organisation's awareness of data protection rules to some extent or a large extent. Generally, EUIBs indicated that the EUDPR has had a positive impact on their data protection policies, and the staff of EUIBs are more aware of their organisation's accountability as data controllers and of the requirements to process personal data.

EUIBs mentioned carrying out data protection impact assessments, identifying and managing data breaches, and considering data protection by design and by default as the main impacts of the EUDPR compared to the repealed Regulation 45/2001. The EUDPR makes the possibility of joint controllership – multiple organisations together defining the purposes of and means for processing personal data – more visible, in the same way as the GDPR. The EDPS has provided guidelines[18] on this topic and the Commission has developed internal templates for joint controllership arrangements.

While the additional accountability requirements necessary for demonstrating compliance with the EUDPR for EUIBs were generally welcomed, some EUIBs noted that the EUDPR rules have led to an increased workload. They also pointed out that the EUDPR sets out relatively complex rules that means more expertise is required in the EUIBs, including among their data protection officers (DPOs), as well as in the networks of data protection coordinators (DPCs) in those EUIBs that have such networks.

All EUIBs, except two of them, keep their records of processing operations in a central register. While this is not a specific requirement under the EUDPR, it is a good practice also recommended

[17] Chapter IX on the processing of operational personal data by EU bodies, offices and agencies when carrying out activities that fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.

[18] Concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, https://edps.europa.eu/data-protection/our-work/publications/guidelines/concepts-controller-processor-and-joint.

by the EDPS[19]. Furthermore, 72% of EUIBs have converted into records all their notifications to the DPO under the previous Regulation[20]. Those that have not yet completed this task should review and update their processing operations documentation to ensure that it is complete and up to date.

3.2 Exercise of data subjects' rights

The EUDPR provides data subjects with a broad set of rights on the processing of their personal data, consistent with the GDPR. The EUIBs as controllers have a specific obligation to make it easy to exercise these rights[21]. As a result, 96% of EUIBs indicated they have conducted awareness-raising activities, such as updating publicly available information on their processing operations, information messages, or guides for data subjects.

A number of EUIBs, such as the Commission, the European Central Bank and the European External Action Service, reported a clear increase in requests received from individuals between 2018 and 2021[22]. However, for others, such as the Court of Justice of the European Union, the European Economic and Social Committee and the European Union Agency for Asylum, the numbers were stable or fluctuated without a clear trend. It is not yet possible to discern a clear trend in the number of requests from data subjects following the entry into force of the EUDPR given the way recording different types of requests varies from one EUIB to another.

3.3 Restricting data subject rights through internal rules

Similar to the GDPR, the EUDPR[23] provides for the possibility of restricting certain data subjects' rights. This can be done by legislative acts and through internal rules[24]. Strict criteria apply to such internal rules. They have to be clear and precise and their application has to be foreseeable to persons subject to them. The rules must be published in the Official Journal and meet the requirements set out in the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms[25].

The restrictions based on internal rules can only relate to the operation of the EUIBs. They must respect fundamental rights, constitute necessary and proportionate measures in a democratic

[19] Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies – Part I: Records and threshold assessment, p. 7, https://edps.europa.eu/sites/default/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf.
[20] Article 25 of Regulation (EC) 45/2001.
[21] Article 14 EUDPR.
[22] This covers general information requests and requests for the exercise of data subject rights under Chapter II of the EUDPR, such as the right to access their personal data held by a EUIB.
[23] Article 25 EUDPR.
[24] This corresponds to the possibilities to restrict data subjects' rights at national level in some Member States, e.g. through ministerial decrees.
[25] Article 25(5) and recital 24 EUDPR.

society and aim to safeguard one of the objectives specifically listed under the EUDPR[26]. Any data subject whose rights have been restricted has the right to lodge a complaint with the EDPS[27].

A large majority (84%) of EUIBs have adopted internal rules. For example, such rules have been introduced to allow deferring providing information to a person concerned in an internal administrative investigation[28]. In others, the objective of such rules has been to ensure continuing effective cooperation with the Member States in those areas where EUIBs activities rely on information received from Member States' competent authorities. For example, internal rules adopted by the Commission for processing personal data in its competition, anti-fraud, and internal audit activities include the possibility of introducing restrictions on data subjects' rights when personal data are obtained from the competent authorities of the Member States[29]. Those rules set out the possibility of imposing similar restrictions when national authorities have imposed restrictions based on a legislative measure possible under the GDPR[30] or the LED[31].

Where EUIBs have adopted internal rules allowing restricting data subjects' rights, they are usually applied on a case-by-case basis as required by their respective internal rules. However, 69% of EUIBs with Article 25 rules in place report that they have not used them yet. Those that have used them have reported less than 10 cases of restrictions, except for the European Parliament and the Commission. The need for restrictions has arisen more often in OLAF's activities, notably for deferring information to data subjects about the processing of their personal data when an investigation is still at an early stage so as not to prejudice the gathering of evidence. OLAF also applied several restrictions regarding data subjects' access requests to their own personal data, which had been rejected only in order to protect rights and freedoms of others[32], e.g. when disclosing the data would put an informant at risk of retaliation.

EUIBs' internal rules usually require them to inform their DPOs of any restrictions applied and to provide DPOs with access to the record and any documents about those restrictions[33].

3.4 Data protection officers

The obligation to have a DPO in every EUIB was already laid down in the previous Regulation 45/2001. The EUDPR has given more visibility to this role by introducing the accountability

[26] Article 25(1) EUDPR.
[27] Article 25(6) EUDPR.
[28] See for example Decision No 59/2021 of the Secretary-General of the Council of the European Union laying down implementing rules concerning the application of Regulation (EU) 2018/1725 of the European Parliament and of the Council and the restriction of data subjects' rights for the purpose of administrative investigations, disciplinary and court proceedings 2022/C 25/02, OJ C 25, 18.1.2022, p. 2–7.
[29] Commission Decision (EU) 2018/1961, OJ L 315/35, 12.12.2018; Commission Decision (EU) 2018/1962, OJ L 315/41, 12.12.2018; Commission Decision (EU) 2018/1927, OJ L 313/39, 10.12.2018.
[30] Article 23 GDPR.
[31] Articles 13(3), 15 or 16 LED.
[32] See Article 2(2) of Commission Decision 2018/1962 referring to the protection of third parties as mentioned in Article 25(1)(h) EUDPR.
[33] This is also recommended in the guidance on Article 25 EUDPR issued by the EDPS, available at: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidance-art-25-regulation-20181725_en.

principle. This means that the controller is responsible for and must be able to demonstrate compliance with data protection rules.

In 46% of EUIBs, their DPOs are supported by networks of DPCs or similar structures[34]. Larger EUIBs are more likely to have such networks (e.g. the European Parliament, the General Secretariat of the Council, the Commission, and the European External Action Service [EEAS]). The EEAS also organises and maintains a network of data protection correspondents in EU Delegations.

A number of EUIBs noted the increase in their DPO's (and by extension DPCs') responsibilities and workload. They acknowledged the need to provide DPOs (and DPCs) with more resources to ensure they can effectively implement their EUIBs' data protection policies. The need to ensure the independence of DPOs was mentioned as well.

There are two trends at play in this context: On the one hand, the EUDPR puts greater emphasis on the controller's accountability, e.g. by removing the prior checking procedure that existed under the previous Regulation 45/2001, thus reducing administrative burden. On the other hand, controllers solicit more guidance from DPOs/DPCs on how best to comply with the EUDPR. In this regard, it was noted that the network of EUIB DPOs has provided an important forum for discussing and clarifying certain legal and technical aspects specific for data processing by EUIBs. This network provides a platform for exchanges between the DPOs and the EDPS and between the DPOs themselves. It cooperates on an ongoing basis and usually meets twice a year.

More than half (54%) of EUIBs have given more resources to their DPOs and data protection functions more generally. Most (84%) of EUIBs have adapted their internal processes to ensure that their staff inform and consult DPOs about new personal data processing operations. This is usually done by including DPOs for instance in change management processes or in project steering boards.

3.5 Data protection impact assessments

The highest number of data protection impact assessments (DPIAs) was carried out by the European Central Bank, the European Investment Bank and the Commission. Compared to the previous system of 'prior checking'[35] under Regulation 45/2001, the number of cases sent to the EDPS has decreased significantly. This was the expected consequence of this change, and reduced consultations of the EDPS on administrative processing operations such as staff appraisal.

[34] For example, the European Commission has a data protection officer attached to the Secretariat-General and is supported by data protection coordinators in every Directorate-General.

[35] Article 27 of Regulation (EC) 45/2001. Under that system, processing operations, e.g. those that involved any processing of personal data related to health and to suspected offences, offences, criminal convictions or security measures or intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct, had to be 'prior checked' by the EDPS. This resulted in a large number of notifications (and corresponding EDPS opinions) on very similar processing operations, e.g. staff selection and appraisal procedures fell under this provision.

Table 1 in the Annex provides an overview of the DPIAs carried out by EUIBs between 2019 and 2021.

Almost all (94%) EUIBs agreed that the EUDPR's criteria[36] for when they have to carry out DPIAs adequately cover high-risk processing operations. Those who disagreed stressed the need for the EDPS to take technological development into account when interpreting these criteria". For example, cloud computing is no longer a 'new' technology and this should be considered when assessing whether DPIAs have to be conducted. The EUIBs that raised this point usually consider that the legal text itself is sufficiently clear, and that this is a matter of interpretation by the EDPS.

The EUDPR contains no specific obligation to publish the results of DPIAs. A large majority (84%) of EUIBs do not publish the DPIAs they have carried out, while 14% publish them in part or as a summary, removing information that could compromise the security safeguards adopted. Only one EUIB indicated that it publishes its DPIAs in full. Publication of DPIAs, where necessary removing information that would put the security of the processing operations at risk, improves transparency regarding EUIBs' compliance with EUDPR rules and is a good practice recommended by the EDPS[37].

3.6 International data transfers

Almost all (91%) EUIBs reported that their activities involve international transfers of personal data. This includes data transfers to non-EU/EEA countries as well as to international organisations. However, several EUIBs mentioned that these transfers are rare or only concern a limited amount of personal data. As regards the transfer tools used, the EUIBs mostly referred to adequacy decisions (adopted under the GDPR[38] or the LED[39]) and contractual instruments, for instance for data transfers to private companies. For data transfers to public bodies, other tools are also used, such as legally binding agreements and administrative arrangements. In addition, 51% of EUIBs mentioned that they carry out limited, occasional transfers, for instance to organise training, based on the statutory grounds for data transfers (the 'derogations')[40].

In practice, data transfers are usually not performed directly by EUIBs, but by their processors (which are not EUIBs) acting on their behalf. The Commission has therefore specifically addressed this scenario in the standard contractual clauses adopted under the GDPR in June 2021[41] to help controllers and processors to comply with the requirements of both the GDPR and the EUDPR. In particular, processors in the European Economic Area (EEA) have the possibility to include these standard contractual clauses for international data transfers in the contracts with their sub-

[36] Article 39 EUDPR.
[37] While the publication of (summary) DPIA reports is not an obligation under the EUDPR, it is a good practice recommended by the EDPS, see Accountability on the ground, Part II, p. 18/19, https://edps.europa.eu/node/4582_en.
[38] Article 45(3) GDPR.
[39] Article 36(3) LED.
[40] Article 50 EUDPR.
[41] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

processors in third countries[42]. This ensures compliance with the EUDPR rules[43] concerning the engagement of sub-processors on behalf of EUIBs, as long as the data protection obligations are aligned in the contracts between: (i) the EUIB and the processor; and (ii) the processor and its sub-processor[44]. In particular, EUIBs can ensure such an alignment by using the standard contractual clauses that have been adopted by the Commission for the relationship between controllers and processors[45].

To provide additional tools ensuring appropriate safeguards for direct data transfers from EUIBs to third countries (i.e. without the involvement of an EU/EEA processor), the Commission is currently developing standard contractual clauses under Article 48(2)(b) of the EUDPR. These clauses will, to the largest extent possible, be aligned with the existing clauses adopted under the GDPR.

Lastly, given the specific questions that arise when personal data are transferred to international organisations (for instance because of the status of international organisations and applicable privileges and immunities), the Commission is working together with EUIB DPOs to develop specific tools (e.g. administrative arrangements) that are adapted to such transfers.

4 EDPS activities

4.1 The EDPS as the data protection supervisory authority for EUIBs

The EDPS is the independent data protection supervisory authority for the EUIBs[46], mirroring the role of the national data protection supervisory authorities established in the Member States under the GDPR and the LED.

Table 2 in the Annex provides an overview of the EDPS supervisory activities from 2018 to 2021. Since the EUDPR entered into force on 11 December 2018[47], the figures for 2018 provide a baseline for comparison with the situation under the previous Regulation 45/2001.

[42] By using 'Module 3' of the standard contractual clauses.
[43] Article 29(4) EUDPR.
[44] See recital 8 of Commission Implementing Decision 2021/914 and footnote 1 of the Annex to that Decision.
[45] Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council.
[46] Except for the Court of Justice of the European Union acting in its judicial capacity, see Article 57(1)(a) and recital 74 EUDPR. In those cases, supervision is carried out by dedicated mechanisms, established by the Decision of the Court of Justice of 1 October 2019 establishing an internal supervision mechanism regarding the processing of personal data by the Court of Justice when acting in its judicial capacity (OJ 2019 C 383, p. 2) and by the Decision of the General Court of 16 October 2019 establishing an internal supervision mechanism regarding the processing of personal data by the General Court when acting in its judicial capacity (OJ 2019 C 383, p. 4). In addition, the Joint Supervisory Authority for the Customs Information System established under Council Decision 2009/917/JHA still exists.
[47] An exception in this regard is Eurojust, for which EUDPR applies since 12 December 2019, see Article 101(2) EUDPR.

The EDPS noted a shift towards EUIBs' core business in the subjects of the consultations received from them since the EUDPR became applicable. This means a shift towards questions on processing personal data for the delivery of tasks assigned to EUIBs in the public interest and away from 'administrative' topics, such as staff management.

The number of inadmissible complaints received by the EDPS has increased between 2019 and 2021[48]. Most of the complaints that were found inadmissible were directed against controllers in Member States, which are not supervised by the EDPS but by their national data protection authorities. The numbers for 2018 were higher most likely because the GDPR became applicable. This led to an increased awareness of data protection rules among the population but also to an increase in inadmissible complaints. The EDPS can also close admissible complaints where an amicable solution has been found.

On inspections and audits, 2019 showed an increase compared to the 2018 baseline, followed by a decrease in 2020 and 2021. This can be explained by the COVID-19 pandemic making on-site checks difficult and them being replaced with remote audits. The EDPS assesses risks to decide which EUIBs to inspect. This takes into account, for instance, the number of consultations submitted, especially when special categories of data are processed as part of a EUIB's core business. The EDPS may also decide to carry out investigations on its own initiative, e.g. on the EUIB's use of cloud service providers.

For data breaches, the EDPS reported that, in the majority of cases, human error was the underlying cause, followed by technical errors and external attacks[49].

The EDPS has used most of its powers under the EUDPR, including for example imposing temporary bans on processing operations[50]. It has not used its new power to issue administrative fines so far, which is a measure of last resort under the EUDPR[51].

The EDPS also pointed out in its contribution to this report that it has invested in awareness-raising activities, such as training, with a peak of more than 4 600 estimated participants in 2019, following the entry into force of the EUDPR. While the numbers of participants in 2020 and 2021 have decreased from that peak, it is still significantly higher than the baseline of the estimated 1 000 participants in 2018.

[48] See table 2 in the Annex.

[49] For 2020 (the latest year with complete statistics): 52% of data breaches were caused by human error; 21% by technical error; 17% by external attack; and the remainder were due to other reasons, e.g. abuse of privileged accounts.

[50] For example, on processing operations for social media monitoring by the then European Asylum Support Office (EASO): https://edps.europa.eu/sites/default/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf. In reply to this, the then-EASO stopped the processing operations at issue.

[51] Under the GDPR, fines can be imposed directly for a breach, e.g. when a controller fails to properly inform data subjects about the processing of their personal data (Articles 12 to 14 GDPR). Under the EUDPR, the EDPS can only impose fines for failure to comply with an order, e.g. to remedy a failure to properly inform data subjects under Articles 14 to 16 EUDPR.

The EUIBs gave largely positive feedback on the interactions with and guidance received from the EDPS, with 86% indicating that replies were always or mostly easy to understand. The EUIBs also appreciated the EDPS's increased contacts with the DPO network.

However, some EUIBs noted that the EDPS's advice sometimes arrived too late[52]. They underlined the importance of continued support and advice from the EDPS and called for timely and practical guidance on certain data protection issues. These issues include implementing the risk-based approach for the controllers, international transfers, and the relationship between controllers (including joint controllers) and their processors.

4.2 The EDPS as adviser to the EU legislator

The Commission formally consults[53] the EDPS, in particular on legislative proposals with an impact on processing personal data, following their adoption by the College[54]. The EDPS replies to these consultations with opinions or comments[55]. The EDPS also issues own-initiative opinions, such as its preliminary opinion on the European Health Data Space[56]. Where a proposal is of particular importance for data protection, the Commission may also consult the European Data Protection Board (EDPB). In that case, the EDPS and the EDPB should issue a joint opinion[57] to ensure that the EU legislator gets consistent advice.

The Commission also consults the EDPS informally before acts subject to consultation requirements are adopted by the College. In reply to such consultations, the EDPS provides informal comments to the Commission. This possibility helps to ensure that Commission acts are fully in line with data protection rules before their adoption. Informal consultations are used particularly for acts which are sensitive or which have more significant impact on data protection.

The activity of the EDPS as an adviser to the EU legislator depends on the number of new proposals prepared by the Commission. Following lower numbers in the last year of the outgoing Commission, the marked increase in formal comments in 2021 is due to the increased number of legislative proposals and the Commission's efforts to ensure a consistent implementation of the obligation to consult the EDPS[58]. This includes implementing and delegated acts that involve processing of personal data. Following the EUDPR's entry into force, the Commission's Secretariat-General produced procedures and raised services' awareness of the requirement to

[52] 67% of EUIBs stated that they received EDPS timely or mostly timely, while 33% were neutral or stated it (mostly) arrived too late.
[53] Article 42 EUDPR.
[54] For implementing and delegated acts, the formal consultation can take place in parallel with the public feedback period for draft implementing and delegated acts.
[55] The EDPS refers to replies on legislative proposals and recommendations under Article 218 TFEU as 'opinions'. Replies concerning implementing or delegated acts are called 'comments', see also Decision of the European Data Protection Supervisor of 15 May 2020 adopting the Rules of Procedure of the EDPS, OJ L 204/49, 26.06.2020, http://data.europa.eu/eli/proc_rules/2020/626/oj.
[56] EDPS Preliminary Opinion 8/2020 on the European Health Data Space, https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-82020-european-health-data-space_en.
[57] Article 42(2) EUDPR.
[58] Article 42 EUDPR.

consult the EDPS. This has resulted in more systematic consultation, including for implementing and delegated acts. For planning purposes, the EDPS and the Commission services hold annual meetings on the upcoming work programme and proposals that will require consultation.

4.3 Cooperation between the EDPS and national data protection authorities

The EDPS is a member of the EDPB and provides it with a secretariat. It also cooperates with national supervisory authorities in exercising their respective tasks in other ways[59]. Examples include referring complaints to the competent data protection supervisory authority or cases involving external service providers that are used both by EUIBs and by controllers subject to the GDPR. The EDPS also actively contributes to the work of the EDPB by taking roles for instance as lead rapporteur or co-rapporteur for guidelines, or otherwise contributing to its work.

Several large-scale IT systems and agencies set up under EU law require that the EDPS and national supervisory authorities, each acting within the scope of their respective responsibilities, actively cooperate to ensure a coordinated supervision[60]. In the past, the establishing acts of each system or agency included specific provisions to that end. The EUDPR[61] creates a harmonised system for this supervision coordination that can be referred to in other acts. This is done for the Internal Market Information System[62], ECRIS-TCN[63], Eurojust[64] and most recently, for Europol[65].

[59] In line with Article 61 EUDPR, the EDPS also cooperates with the Joint Supervisory Authority established under Article 25 of Council Decision 2009/917/JHA.

[60] Examples include the Schengen Information System, the Visa Information System and Eurodac. See Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312, 7.12.2018, p. 56–106); Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ L 218, 13.8.2008, p. 60–81); and Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 180, 29.6.2013, p. 1–30.

[61] Article 62 EUDPR.

[62] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012, OJ L 295, 21.11.2018, p. 1–38.

[63] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ L 135, 22.5.2019, p. 1–26.

[64] Article 42(2) of Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018, p. 138–183.

[65] See changes to Article 44(2) of the Europol Regulation introduced by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation

Other systems still have supervision coordination groups with detailed rules in their establishing acts, or detailed references to meetings as part of the EDPB[66].

The EDPS also contributes to the Schengen evaluation mechanism set up under Council Regulation 1053/2013[67]. Under that Regulation, the Commission may invite the EDPS to designate an observer to take part in an on-site visit concerning an area covered by its mandate, i.e. data protection evaluations[68]. This corresponds to the possibility for Frontex and Europol to designate observers for evaluations of border management and police cooperation respectively. In the Commission's view, the expertise of EDPS observers is a valuable asset to data protection evaluations.

4.4 EDPS resources

The number of EDPS staff (including the EDPB secretariat[69]) has steadily grown over the reporting period[70], reflecting the overall trend in national data protection supervisory authorities. The EDPB secretariat's activities have increased over time with a growing output of EDPB guidelines, recommendations, opinions, and other documents to which the secretariat contributes. Providing sufficient resources for the EDPB secretariat is essential given the stronger role it is expected to have in effectively enforcing the GDPR. This concerns in particular the EDPB's objective to develop closer cooperation on strategic work and to use new tools supporting cooperation between data protection authorities[71]. In particular, having a strong and well-resourced secretariat to support the work of the EDPB is critical for ensuring that the EDPB can deliver its work as required, notably in the context of the consistency mechanism[72], the use of which is expected to continue growing.

with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, OJ L 169, 27.6.2022, p. 1–42.

[66] Article 57 of Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L 312, 7.12.2018, p. 14–55 and Article 71 of Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312, 7.12.2018, p. 56–106.

[67] Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen *acquis* and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen, OJ L 295, 6.11.2013, p. 27–37.

[68] Article 10(5) of Council Regulation (EU) No 1053/2013 of 7 October 2013.

[69] Article 57(1)(l) EUDPR.

[70] See table 4 in the Annex.

[71] EDPB statement on closer cooperation on strategic files, 29 April 2022: DPAs decide on closer cooperation for strategic files | European Data Protection Board (europa.eu).

[72] Chapter VII GDPR.

In its contribution to this report, the EDPS considered, in particular, that should it be entrusted with additional tasks, e.g. as a market surveillance authority under the artificial intelligence legislative proposal[73], it should be provided with corresponding additional resources.

5 Commission's use of empowerments to adopt delegated and implementing acts

The EUDPR contains several empowerments for the Commission to adopt implementing acts and lay down standard clauses, as well as cross-references to empowerments under the GDPR[74].

The EUDPR[75] contains provisions empowering it to lay down standard data protection contractual clauses for controller-processor contracts, corresponding to the empowerment in the GDPR[76]. The Commission used this empowerment and adopted standard contractual clauses covering controller-processor relationships in June 2021[77] covering both the GDPR and the EUDPR. These clauses provide easy-to-use tools for controllers to effectively manage relationships with their processors.

The EUDPR[78] also empowers the Commission to adopt standard data protection contractual clauses for providing appropriate safeguards for the transfer of personal data outside the EU/EEA. The Commission is currently preparing such clauses.

6 Data protection rules for bodies and agencies dealing with police cooperation and judicial cooperation in criminal matters

Chapter IX of EUDPR contains rules for EUIBs processing operational personal data when carrying out activities in the scope of police cooperation and judicial cooperation in criminal matters ('law enforcement chapter'). It aims to reduce fragmentation:

- between data protection regimes applicable to processing operational data by EU agencies in this field;
- with the data protection regime applicable to national criminal law enforcement activities under the LED.

To this end, the EUDPR law enforcement chapter provides a set of horizontal rules based on the LED. These rules can be supplemented, where necessary, by specific rules in the agencies'

[73] COM/2021/206 final.
[74] See Article 47 EUDPR enabling EUIBs to rely on adequacy decisions adopted under the GDPR and the LED and Article 14(8) EUDPR on delegated acts on icons under Article 12(8) GDPR.
[75] Article 29(7) EUDPR.
[76] Article 28(7) GDPR.
[77] Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (Text with EEA relevance), OJ L 199, 7.6.2021, p. 18–30, https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32021D0915.
[78] Article 48(2)(b) EUDPR.

founding acts, depending on their respective mandates and on the specific nature of their tasks and data processing operations.

The EUDPR states the need to ensure a uniform and consistent protection of natural persons when processing their personal data[79]. To that end, it points explicitly to the objective of extending the application of the EUDPR law enforcement chapter to agencies that had separate data protection frameworks in their establishing acts when the EUDPR was adopted, namely Europol and the European Public Prosecutor's Office (EPPO). It also refers to the possible amendment of the law enforcement chapter, if required.

6.1 Extending the application of the EUDPR's law enforcement chapter

At the time of writing, the EUDPR law enforcement chapter applies to processing operational personal data by:

- Eurojust[80], complemented by specific rules included in the Eurojust Regulation;
- Europol[81], complemented by specific rules included in the Europol Regulation, which has been amended[82] since the EUDPR's entry into force;
- Frontex for the small part of its activities that are part of criminal law enforcement[83].

However, the EUDPR law enforcement chapter does not yet apply to the EPPO whose establishing Regulation was adopted before the EUDPR. The EPPO Regulation provides for a standalone regime for processing operational data. This has two consequences: First, some provisions in the EPPO Regulation differ in substance from the EUDPR law enforcement chapter, such as the processing of 'restricted' personal data[84]. Second, some provisions of the EPPO Regulation, although similar in substance, are worded differently than the EUDPR law enforcement chapter, which could lead to different interpretations.

---

[79] Article 98(2) EUDPR.

[80] Article 26 of Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018, p. 138–183.

[81] Article 28 of the amended Europol Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/.

[82] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, OJ L 169, 27.6.2022, p. 1–42.

[83] See Articles 10(1)(q) and 90 of Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, OJ L 295, 14.11.2019, p. 1–131, https://eur-lex.europa.eu/eli/reg/2019/1896/oj.

[84] Article 61(4) of the EPPO Regulation allows the processing of 'restricted' data for 'with the exception of storage, only […] for the protection of the rights of the data subject or another natural or legal person who is a party of the proceedings of the EPPO, or for the purposes [of evidence]'. The corresponding Article 82(3) of the EUDPR states that 'restricted data shall be processed only for the purpose that prevented their erasure', which includes maintaining the data for evidence, but does not refer to the protection of the rights of the data subject or others.

In the interest of consistency and in line with the general objective of minimising the fragmentation of data protection rules, a similar approach to the one adopted for Eurojust and Europol should be followed for the EPPO. The objective is to ensure the direct applicability of the EUDPR law enforcement chapter to the EPPO, keeping only necessary specifications in the EPPO Regulation. At the same time, given that the EPPO has been operational for only one year, in the short term, it is still necessary to gather more insight into the practical application of the EPPO data protection regime. This will enable precisely identifying those specifications, taking into account the nature of the EPPO as the EU's independent public prosecution office[85].

6.2 Clarifying the applicability of certain EUDPR provisions to the processing of operational data

The EUDPR[86] states that 'only Article 3 [definitions] and Chapter IX [law enforcement chapter] of this Regulation shall apply to the processing of operational personal data'.

The law enforcement chapter contains substantive provisions corresponding to most provisions of Chapters II to V of the EUDPR (general principles, rights of data subjects, certain obligations of controllers and processors, international data transfers), with some differences to take the specific nature of law enforcement into account (e.g. rules on informing data subjects and on their right of access to their data).

It is important to clarify, by amending the EUDPR, that the law enforcement chapter lays down specific rules only to the corresponding provisions of other chapters of EUDPR that have a direct equivalent in the law enforcement chapter . This way, if the legislator does not include specific rules in an agency's establishing act, the provisions in chapters other than the law enforcement chapter that have no direct equivalent in the latter[87] apply to the processing of operational data.

This amendment would improve legal certainty and would provide a complete framework (e.g. on the position of DPOs, cooperation with national data protection supervisory authorities), including for any future agencies in this field[88]. Having such a complete framework would also reduce the risks of fragmentation.

[85] The experience gained with Eurojust and Europol is not directly transferable to the EPPO, given that the EPPO's mandate is not to support and enhance cooperation among national authorities but to investigate and prosecute crimes affecting the EU's financial interests.
[86] Article 2(2) EUDPR.
[87] E.g. regarding controllers' duty to cooperate under Article 32 EUDPR, the rules on data protection officers in Articles 43 to 45 EUDPR, Article 31 on keeping records of processing activities, and on cooperation with other supervisory authorities under Article 61 EUDPR.
[88] The specific legal framework of these agencies would still need to be laid down in line with the requirements of the EUDPR, e.g. Article 72 on defining storage periods. But there would be no need to regulate data subject rights or the powers of the EDPS, unless the legislator would specifically choose to deviate from the approach of the EUDPR.

6.3 The EDPS's powers in supervising EU bodies and agencies

Currently, the regulations establishing the EPPO, Eurojust, and Europol contain specific provisions on the powers of the EDPS[89].

The updated Europol Regulation gives powers to the EDPS that are aligned with those under Article 58 of the EUDPR[90]. This is notably the case for the power to issue administrative fines and the power to order the controller or processor to bring processing operations into compliance, where appropriate, in a specified manner and within a specified period.

However, in the case of EPPO the powers of EDPS are formulated differently than in the EUDPR. The EDPS does not have the two powers mentioned above[91].

The Frontex Regulation, for the small part of Frontex' activities subject to the law enforcement chapter[92], does not include any specific provisions on the EDPS's powers, leading to uncertainties about those powers.

Providing the EDPS with the full range of powers set out under Article 58 of the EUDPR could be achieved by following the two steps below.

1. Clarifying that the EUDPR, as a default option, entrusts the EDPS with the supervision of the law enforcement chapter and with the powers granted to it under Article 58 of the EUDPR[93]. This requires amending the EUDPR as proposed in the previous section. This would also address the gap in the Frontex Regulation.

2. By removing the provisions on the EDPS's powers from the founding acts of the agencies and bodies, the full range of the EDPS's powers under the amended EUDPR would apply directly to Eurojust and the EPPO. The objective is to align them as much as possible to reduce fragmentation of data protection rules.

7 Way forward

Overall, the EUDPR is working well and is fit for purpose. At this stage the Commission will not propose amendments on those parts that are equivalent to the corresponding rules in the GDPR,

[89] Article 85 of the EPPO Regulation, Article 40 of the Eurojust Regulation and Article 43 of the Europol Regulation.
[90] Certain EDPS tasks that are not relevant for Europol, e.g. approving standard contractual clauses, are not repeated.
[91] Under Article 85(3)(b) of the EPPO Regulation and Article 40(3)(b) of the Eurojust Regulation, in the event of an alleged breach of the provisions governing the processing of operational personal data, the EDPS can only refer the matter to the EPPO or Eurojust, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects.
[92] See Articles 10(1)(q) and 90 of the Frontex Regulation.
[93] Article 1(3) EUDPR gives the EDPS the task to 'monitor the application of the provisions of this Regulation to all processing operations carried out by a Union institution or body'. Although this provision can be interpreted as applying also to the activities falling under the law enforcement chapter, it would be useful to make it explicit to ensure legal certainty.

thus maintaining the closest possible alignment between the EUDPR and the GDPR[94]. The possible amendments considered in this report concern other parts, notably the relation of the EUDPR's law enforcement chapter to the other provisions of this Regulation.

In spring 2022, the Commission proposed rules to strengthen information security in the EUIBs[95], which will have a positive impact on information security, including on the protection of personal data. That proposal aims to further improve EUIBs' resilience and ability to respond to incidents when faced with cybersecurity threats.

The Commission will also take the steps outlined in the points below:

- when updating the establishing acts for large-scale IT systems that still include detailed rules on a supervision coordination model, ensure that the EUDPR's supervision coordination model[96] will apply in order to streamline procedures;
- consider amendments to the EUDPR in order to:
    - improve legal certainty and complete the framework for the processing of operational data by clarifying in Article 2(2) that the general provisions of the EUDPR also apply to processing operational personal data, unless the law enforcement chapter contains specific provisions (such as on the right of access). This would also provide a ready-made framework for any future agencies in the fields of judicial cooperation in criminal matters and police cooperation;
    - ensure the participation of the EDPS as observer in all data protection evaluations under the Schengen evaluation mechanism;
- subsequently, consider amending the EPPO and Eurojust Regulations in a future revision to ensure the full application of the rules on processing operational personal data in the amended EUDPR, taking the specific nature of those bodies into account. This will also lead to harmonising the EDPS' powers over these bodies and agencies with those it has over the other EUIBs;
- propose standard contractual clauses for international transfers of personal data[97] for the EUIBs;
- continue the close cooperation with the EDPS (and, where relevant, the EDPB) to ensure a timely and targeted consultation on new proposals[98] and also continue to consult the EDPS informally on important texts before they are adopted.

[94] Should the GDPR be amended at a later stage, the Commission will consider the necessary amendments to the EUDPR to keep both texts aligned.
[95] Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, COM(2022) 122 final.
[96] Article 62 EUDPR.
[97] Under Article 48(2)(b) EUDPR.
[98] In line with Article 42 EUDPR.

The EDPS is invited to:

- provide additional and timely practical guidance to the EUIBs, including on international data transfers;
- continue raising awareness of controllers and processors about their obligations under EUDPR, as well as advising DPOs;
- intensify efforts to effectively enforce the EUDPR to ensure the full protection of data subjects.

EU institutions, bodies, offices and agencies are invited to:

- continue and, when necessary, step up awareness-raising efforts to ensure a sufficient level of in-house expertise on EUDPR rules;
- consider publishing DPIAs, excluding information that could compromise the security safeguards adopted where necessary;
- ensure that DPOs (as well as DPCs) have sufficient resources and a position within the EUIBs that enable them to carry out their tasks efficiently and independently;
- finish converting their remaining notifications under the previous data protection regulation into data protection records.

ANNEX

Table 1 – Data protection impact assessments and prior consultations carried out by EUIBs

	2019	2020	2021
Residual risk accepted	30	50	77
EDPS prior consultation	3	3	5
Project abandoned	2	2	0

Table 2 – EDPS supervisory activities

	2018	2019	2020	2021
Consultations	50[99]	75	59	52
Prior consultations	0	0	1	4
Transfer authorisations	0	1	0	4
Admissible complaints received	58	59	43	44[100]
Decisions[101] on admissible complaints	23	48	35	22
Inadmissible complaints received	240	151	203	269
Inspections/audits carried out	5	9	4	4
Formal investigations carried out	0	4	1	2
Data breach notifications received	7	95	121	82[102]

[99] Two of which followed the entry into force of EUDPR.
[100] Until 15 November 2021.
[101] Including cases closed by amicable settlement, referral to DPO and other means of closure.
[102] Until mid-November 2021.

Table 3 – EDPS advisory activities

	2018	2019	2020	2021
Comments	13	3	19	72
Opinions	7	6	8	12
Own-initiative opinions	1	1	2	0
Joint opinions with EDPB	0	1	0	5
Informal comments	33[103]	16	13	25

Table 4 - EDPS resources

	2018	2019	2020	2021	2022 (estimated)
Total number of EDPS staff (including the EDPB secretariat)	98	100	118	126	139
EDPS staff in EDPB secretariat	19	22	27	34	38
Budget[104]	EUR 13 539 302 (executed)	EUR 15 301 687 (executed)	EUR 14 211 7 19 (executed)	EUR 16 761 285 (executed)	EUR 20 202 000 (draft)

[103] Under the previous Regulation 45/2001, the EDPS counted consultations on delegated/implementing acts under 'informal' comments. A certain amount of the comments listed under informal comments for 2018 would have been counted under 'formal comments' in later years.

[104] These numbers have been updated compared to the numbers in the EDPS contribution to this report.