COUNCIL OF THE EUROPEAN UNION

Brussels, 4 June 2014 (OR. en)

10595/14

DATAPROTECT 89
EDPS 4
DAPIX 79
FREMP 113
JAI 428
POLGEN 83

NOTE

From:	European Data Protection Supervisor
To:	Delegations
Subject:	The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience - Policy paper

Delegations find in Annex the above policy paper.

Executive Summary

This policy paper explains, on the basis of ten years of experience, how the European Data Protection Supervisor (EDPS) advises the EU institutions on policy and legislation.

The EDPS is the independent data protection authority of the European Union. We monitor and ensure the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals and we advise the EU institutions on proposals for legislation and new policies.

Since the EDPS was established in 2004, major changes in the legal, economic and technological context have occurred. The entry into force of the Lisbon Treaty has confirmed data protection as a general principle of EU law (see mainly Article 8 of the Charter and Article 16 TFEU), and a number of landmark decisions handed down by the European Court of Justice have underlined the importance of privacy and data protection as an integral part of the decision making by the EU's legislature.

Under Article 28(2) of the Regulation, the Commission has an obligation to consult the EDPS whenever it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. The scope of this obligation is broad. Under Article 41 of the Regulation the EDPS is responsible for ensuring that the fundamental rights and freedoms of individuals, and in particular their right to privacy, are respected, and for advising EU institutions and bodies "on all matters concerning the processing of personal data", and under Article 46(e) we monitor developments that may have an impact on the protection of personal data.

In line with established practice, the EDPS is also consulted *informally* before such proposals are adopted by the Commission. We engage constructively with the European Parliament, the Council and the Commission and remain available to provide targeted and timely advice at any stage of the EU decision-making process. We act selectively on the basis of the priorities set out in our Strategy, the Annual Management Plan, and our inventory. Consequently, we focus our attention and efforts on areas that present the highest risk of non-compliance or where the impact on privacy and data protection are greatest. In order to maximise the impact and usefulness of our work, we are developing **a 'policy toolkit'** – which includes general guidance to the legislator, for instance through thematic or sectoral **guidelines** – in order to help the institutions to make informed decisions on the data protection impacts of new proposals. For example, we envisage writing a **background paper on necessity and proportionality**.

The strategic objective underlying the interventions by the EDPS is to ensure that both the European Commission, as most frequent initiator, and the European Parliament and the Council as the co-legislators are aware of data protection requirements and integrate data protection in new legislation. We aim to develop a culture of accountability whereby these institutions recognise their own responsibility to ensure the protection of personal data when developing new EU policies. To this end, we are ready to conclude a **Memorandum of Understanding** with the three main institutions which would set out how in practice we can add value in the EU legislative process through exercising our advisory role.

Contents

The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience

1. Introduction

This policy paper[1] explains, 10 years on from the establishment of the institution, how the EDPS advises the EU institutions on policy and legislation. It updates and replaces a previous paper on this subject, which was adopted on 18 March 2005 and was meant to set the scene for the consultative activities of the EDPS which have developed since.[2] This policy paper is addressed to all our stakeholders and interlocutors in the EU's policy making process, including colleagues within the institutions and bodies of the EU insofar as they deal with files that are relevant for data protection, and national data protection authorities who are members of the Article 29 Working Party.

The role of the EDPS as an advisor to EU institutions and bodies should be seen in light of the growing importance of the protection of fundamental rights within the EU legal order, the need for consistency as a constitutive element of an effective data protection, as well as the results of the strategic review conducted by the EDPS in 2011-2012, as reflected in our Strategy for the Period 2013-2014 ("Strategy"). Opinions covering a wide range of EU policy areas[3] are the most visible expression of this role, which we exercise in accordance with our Rules of Procedure[4] ("EDPS RoP").

---

1 Under Article 16 of the EDPS Rules of Procedure, the EDPS adopts policy papers to provide guidance on how specific activities are to be carried out.

2 "The EDPS as an advisor to the Community institutions on proposals for legislation and related documents", adopted on 18 March 2005, available on the EDPS website.

3 See EDPS website under "Consultation".

4 OJ 2013, L 273, 15.10.2013, p.41.

2. The legal context

The EDPS acts as an independent authority[5] under Article 8(3) of the Charter of Fundamental Rights of the European Union ("Charter"). Our consultative role is laid down in a number of provisions of Regulation 45/2001[6], in particular in Articles 28(2), 41 and 46 thereof. Under Article 28(2), consultation of the EDPS is a compulsory element of the ordinary legislative procedure and of specific procedures in the Treaties, where the Commission adopts a legislative proposal. Article 28(2) should be read in connection with Article 41 of the Regulation, according to which the EDPS is responsible for ensuring that the fundamental rights and freedoms of individuals, and in particular their right to privacy, are respected, and for advising EU institutions and bodies "on all matters concerning the processing of personal data"[7].

---

5 On the need for the complete independence and for sufficient powers of the data protection authorities in relation to their various roles, see Case C-518/07 *Commission* v *Germany*, judgment of 9 March 2010; Case C-614/10 *Commission* v *Austria*, judgment of 16 October 2012; Case C-288/12 *Commission* v *Hungary*, judgment of 8 April 2014.

6 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.

7 In the Orders in Cases C-317/04 and C-318/04 *PNR*, the Court confirmed that this concept has a broad scope, stating explicitly that the "advisory task does not cover only the processing of personal data by those institutions or organs".

Since the EDPS was established in 2004, major changes in the legal, economic and technological context have occurred. Following the entry into force of the Lisbon Treaty, the fundamental rights to privacy and to the protection of personal data have been reinforced in the EU legal order (see mainly Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the EU – "TFEU"), a number of landmark decisions handed down by the European Court of Justice have underlined the importance of privacy and data protection as integral part of the decision making by the EU's legislature[8] and this has been reflected in the ongoing reform of the legal framework on data protection[9].

[8] See e.g. Joined Cases C-92/09 and C-93/09 *Schecke and Eifert*, judgment of 9 November 2010, and most recently Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, judgment of 8 April 2014.

[9] Communication from the Commission of 25 January 2012 "Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century", COM(2012) 9 final; Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final; Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final.

3. The advisory role of the EDPS: building on ten years of experience

In the past decade, we have followed closely the drafting of major EU data protection instruments, sometimes issuing successive contributions at different stages of the legislative procedure[10]. We also provided contributions to the most important legislative and policy files with data protection implications[11]. On the basis of this experience and in the spirit of efficient use of resources, we are currently in the process of developing a new **'policy toolkit'** – including thematic or sectoral **guidelines**[12] – in order to both help the legislator to make informed decisions on the data protection impacts of new proposals in line with the main principles set out in part 4 below and to improve the focus in our consultation.

In our role as advisor, we rely not only on the experience we built up in advising the institutions but also on our expertise acquired in the field of supervision. These two main roles are complementary, and we strive to take advantage of the synergies between them and to ensure consistency between the principles advocated in our policy and our supervisory work.

---

10 For instance, we issued three separate opinions on the (draft) Framework Decision 2008/977 FD on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters; two opinions on the last revision of Directive 2002/58/EC on privacy and electronic communications, and multiple interventions on the (still ongoing) data protection reform package.

11 P. de Hert and V. Papakonstantinou, "The EDPS as a unique stakeholder in the European data protection landscape, fulfilling the explicit and non-explicit expectations", in *Data protection Anno 2014: How to Restore Trust?*, Intersentia 2014, p. 249.

12 For example, sectoral guidelines on data protection in the field of financial services will be adopted in 2014.

3.1. Our core values and guiding principles

According to our Strategy[13], we are guided in our work by the core values of impartiality, integrity, transparency and pragmatism. These are implemented in the following manner:

- ***Impartiality:*** *working within the legislative and policy framework given to us, being independent and objective, finding the right balance between the interests at stake.*
  - Throughout the legislative process, we engage constructively with the European Parliament, the Council and the European Commission, maintaining an equal distance from each of the three institutions.
  - Impartiality is also a guiding principle when we choose to act, where appropriate also in a proactive manner.

- ***Integrity:*** *upholding the highest standards of behaviour and doing what is right even it is unpopular.*
  - We advise on clear legislative drafting to ensure that data protection issues are addressed in an unambiguous and consistent manner.
  - We provide our advice in a timely manner so as to be useful at the appropriate stages of the legislative process.
  - On substance, we provide consistent advice in an appropriate format. For legislative proposals of the Commission, with an impact on data protection, we will normally issue formal Opinions.
  - We apply the principle of selectiveness and set out priorities in our Inventory[14]. In particular, we focus our attention and efforts on areas that present the highest risk of non-compliance or where the impact on privacy and data protection are greatest.
  - We aim to provide relevant and authoritative advice based on the unique expertise developed over the past ten years in data protection law and practice - including supervision - and of relevant technology.

[13] Strategy, p. 15.
[14] See section 5 below.

- ***Transparency:*** *explaining what we are doing and why, in clear language that is accessible to all.*
    - We build on an annual Inventory, an instrument that ensures that our choices whether or not to intervene are consistent and transparent for our stakeholders.
    - We cooperate constructively both with the EU institutions and with other data protection authorities, supervisory bodies, international organisations and other stakeholders, seeking consistency and high standards in data protection across the EU.
    - In procedural terms, we strive to be available at any time and for any stakeholder to help identify solutions.
    - We explain complex technical issues in a way that is understandable for non-specialists, while at the same time remaining technically and scientifically correct.

- ***Pragmatism:*** *understanding our stakeholders' needs and seeking solutions that work in practice.*
    - We give objective advice, based on analysis, not on perceptions.
    - We rely on our experience in our supervisory role to recommend solutions that are workable in practice. We work to find practical solutions, particularly in complex policy areas which may require difficult balances to be struck.
    - We seek to ensure that data protection will be an integral part of policy-making and legislation, whilst ensuring a fair balance with other public interests and fundamental rights.

The strategic objective underlying these values is to ensure that both the European Commission, as most frequent initiator, and the European Parliament and the Council as the co-legislators are aware of data protection requirements and integrate data protection in new legislation[15]. We aim to develop a culture of accountability whereby these institutions recognise their own responsibility to ensure the protection of personal data when developing new EU policies.

[15] Strategy, p. 11.

To this end, we are ready to conclude a **Memorandum of Understanding** with the three main institutions (Parliament, Council and the Commission) which would set out how in practice we can add value in the EU legislative process through exercising our advisory role.

3.2. The broad scope of our advisory role

In all areas. In line with Article 28(2) of the Regulation, any legislative proposal that includes provisions on the processing of personal data, which builds on, supplements or amends the existing legal framework for data protection, or which has a significant impact on the protection of individual's rights and freedoms with regard to the processing of personal data should be subject to consultation of the EDPS. In other words, a legislative proposal does not need to have direct impact on the EU data protection rules themselves in order to trigger scrutiny by the EDPS. Accordingly, over the years, we have covered a wide number of policy areas.

Proactive. Our role as a general advisor on all data protection matters at EU level, means that we not only advise in reaction to a consultation from the Commission (or to a request for advice by another institution), but also on our own initiative, when a matter is of significant importance in this area. In addition, in areas of intense legislative activity or particularly significant impact on personal data protection, we develop general guidance in thematic or sectoral guidelines or other appropriate instruments.

At all stages. In order to best achieve our awareness-raising goals and to improve the quality of EU policies, we are prepared to provide advice at any stage of the legislative process, from the earliest phases of policy making until discussions in Parliament and Council at different stages of the EU law-making process. In some cases, this may imply intervening more than once in the various procedural steps.

To multiple stakeholders. Through our opinions, comments and other forms of intervention, we aim at raising awareness of data protection issues, not only within the EU institutions and bodies, but also towards the general public[16].

[16] See below, section 6.5 "Transparency and confidentiality".

Assessing (technological) complexity. The impact of a legislative proposal on the protection of personal data is not always evident, especially given the technical nature of data processing, the impact of information technology and the complexity of many legislative files. To respond to this challenge, we have the necessary IT technical expertise and insight to monitor technological developments and assess their impacts on data protection and privacy.

4. Analysing the impact on privacy and data protection

This section outlines in broad terms how we assess, in light of the case law of the Court of Justice, the impact of proposed measures on the rights to privacy and the protection of personal data[17].

4.1. Are personal data being processed?

When our stakeholders are considering involving the EDPS in a legislative or policy making procedure, the first question they have to answer is whether a (proposed) instrument implies the processing of personal data.

Processing of personal data encompasses any operation, automatic or not, such as collection, recording, storage, use, disclosure, transmission or otherwise making available of any information relating to an identified or identifiable natural person[18].

[17] This can be read alongside the "fundamental rights checklist" proposed in the Commission's Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM(2010) 573.

[18] Articles 2(a) and (b) common to Directive 95/46/EC and Regulation 45/2001.

In consequence, the concept of "personal data" covers much more than information that directly identifies an individual, such as a name[19], a national registration number or taxpayer identification number. According to the Court of Justice, the concept of personal data also covers, among other things: information related to remuneration[20], amounts of agricultural subsidies received[21], biometric information[22], IP addresses[23], traffic and location data[24], amount of earned or unearned incomes and assets of natural persons[25], daily work periods, rest periods and corresponding breaks and intervals[26]. In this context, we would refer to Opinion 4/2007 of the Article 29 Data Protection Working Party, which provides a thorough analysis and multiple examples[27]. In particular, the Opinion analyses the four main elements of the definition, i.e. "any information", "relating to", "identified or identifiable" and "natural person", each of which needs to be assessed to determine whether "personal data" are at stake in any given situation.

4.2. EU law on privacy and data protection

Where a proposed legislation or other measure involves the processing of personal data, it must comply with primary EU law, and in particular with Articles 7 and 8 of the Charter. In many cases the right to privacy under Article 7 of the Charter will be applicable; but in all cases, the right to data protection will be applicable.

Articles 7 and 8 are closely linked, but are different in nature and lay down distinct requirements which must be met in order to ensure compliance.

---

19 Case C-101/01, *Lindqvist*, judgment of 6 November 2003, paragraph 24; Case C-553/07 *Rijkeboer*, judgment of 7 May 2009, paragraph 42.

20 Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof* and *Österreichischer Rundfunk*, judgment of 20 May 2003, paragraph 64.

21 *Schecke*, note 8 above, paragraph 60.

22 Case C-291/12, *Schwarz v Stadt Bochum*, judgment of 17 October 2013, paragraph 27.

23 Case C-70/10 *Scarlet Extended v. SABAM*, judgment of 24 November 2011, paragraph 51.

24 *Digital Rights Ireland*, note 7 above, paragraphs 26 and 29.

25 Case C-73/07 *Satakunnan Markkinaporssi and Satamedia*, judgment of 16 December 2008, paragraphs 35 and 37.

26 Case C-342/12 *Worten* v *Autoridade para as Condições de Trabalho ACT*, judgment of 30 May 2013, paragraph 19.

27 Opinion 4/2007 on the concept of personal data, WP136, adopted on 20 June 2007.

Article 7 can be seen as a classic fundamental right that protects individuals primarily against interference by the State. Article 7 generally corresponds to Article 8 of the European Convention on Human Rights (ECHR). Article 7 must be read in conjunction with Article 52(1) of the Charter[28], which allows limitations to fundamental rights, provided that such limitations, in addition to being provided for by law:

- respect the "essence" of the right(s);

- genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others; and

- subject to the principle of proportionality, are necessary.[29]

The Court of Justice has further specified that legislators have to consider whether these objectives can be achieved with less intrusive measures[30]. It also follows from the case law that limitations of fundamental rights must be interpreted in a restrictive way[31]. Within these constraints, the EU legislator remains free to make political choices. However, judicial review of any exercise of that discretion is likely to be particularly strict in the context of mass data processing affecting a very large number of persons, as well as the access to and use of such data by law enforcement authorities[32].

---

28 With regard to the fundamental rights to privacy and data protection, see for example *Digital Rights Ireland*, note 8 above.

29 Article 52(1) follows Article 8(2) of the ECHR which establishes that there shall be no interference by a public authority with the exercise of the right to privacy except such as is in accordance with the law and if necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others

30 *Schecke*, note 8 above, para. 81.

31 *Satamedia*, note 26 above, para. 56, *Schecke*, note 8 above, para. 77 and 86.

32 *Digital Rights Ireland*, note 8 above, paras. 57-61.

Article 8, in contrast, must be seen as a proactive horizontal right to protection that is not limited to interferences by the State. Article 8 gives individuals the right that their personal data can only be processed if certain conditions are met. Their personal data can only be processed – not only by the State, but by any other actor – if the standards set out in paragraphs 2 and 3 of Article 8 are met, i.e. (i) the processing is fair and lawful, for specified purposes, (ii) transparency is ensured by giving the individuals rights to access and correction, and (iii) control by an independent authority is ensured. These principles are developed in various instruments of EU data protection law, in particular in Directive 95/46/EC, Regulation 45/2001, Framework Decision 2008/977/JHA and Directive 2002/58/EC. Compliance with Article 8 of the Charter must therefore be assessed by specific reference to the system of safeguards laid down in those instruments. These rules are the benchmark for the legislator, and any derogations from those rules should in general be avoided or, at the very least, appropriately justified.

4.3. Analytical steps

When assessing a proposed measure which includes the processing of personal data, a number of analytical steps should be followed:

1. What is the **legal ground** for the data processing? According to Article 8(2) of the Charter this could be the consent of the person concerned or another legitimate basis laid down by law. This is further specified in Article 7 of Directive 95/46/EC and Article 5 of Regulation 45/2001. Where relevant, account should also be taken of Article 7 and other relevant provisions of the Charter.

2. Is the "**essence"** of the right (that is, the basic identity or substance of a right which makes it meaningful) respected? A measure may impact seriously on a right, but still respect its essence[33]. For example, the Court has held that the retention of traffic and location data under Directive 2006/24/EC constituted a serious interference with the right to privacy but that, as it did not apply to the content of electronic communications, it did not *per se* adversely affect the essence of the right to privacy.

[33] *Digital Rights Ireland*, note 8 above, paras. 39-40.

3. Is the proposed measure **sufficiently precise**? Are the rules governing the scope and application of the measure clear and precise? Is it explicitly specified what sort of data will be gathered, processed or exchanged and by whom?

4. Is the objective of the proposed measure sufficiently clear? Is the **purpose of the processing** explicitly and specifically described? If further processing is envisaged, is its purpose **compatible** with the original one, and if not, are there sufficient grounds for a restriction?[34]

5. Is the data processing envisaged by the measure **adequate, relevant and not excessive** in relation to the purposes for which they are collected or further processed?

6. Is the choice of the proposed measure appropriate? Could any other, less intrusive measure achieve the desired outcome with less interference with the fundamental right at stake? This is related to the **proportionality** test, which is further explained below.

7. Where a measure aims at protecting **other public interests or fundamental rights**, how are those interests or rights balanced with privacy and data protection?

8. If there is a serious impact on a fundamental right and in addition to the previous points, are **appropriate safeguards** provided at EU level (as opposed to simply leaving them to Member States to determine).

9. Are there sufficient guarantees that data subjects can exercise their **rights to access and correction**, as well as other relevant rights?

10. Is it sufficiently guaranteed that compliance of the data processing with data protection law can be effectively **controlled by an independent authority**[35]?

---

[34] This is the so-called purpose limitation principle, currently set out in Article 6(1)(b) of Directive 95/46/EC and Article 4(1)(b) of Regulation 45/2001. See also Article 13(1) of Directive 95/46/EC and Article 20(1) of Regulation 45/2001 for possible restrictions.

[35] *Commission* v *Germany*, para. 23; *Commission* v *Austria*, para. 37; *Commission* v *Hungary*, para. 47 (all note 5 above). In *Digital Rights Ireland*, note 8 above, para. 68, the Court stated that in the circumstances of the case such independent supervision is not fully ensured where the measure in question does not require processed data to be stored within the EU.

11. Where complex IT-systems are involved, are the need for **security** and the principles of **data protection by design and data protection by default** sufficiently taken into account?

4.4. The concept of proportionality

As indicated in item 6 above, policymakers must assess the proportionality of the measure. Proportionality may be understood as that which is "appropriate for attaining the legitimate objectives pursued by the legislation at issue and [does] not exceed the limits of what is appropriate and necessary in order to achieve those objectives"[36].

In assessing proportionality under Article 52(1) of the Charter, the Court has applied a stricter test in rulings such as *Schecke*[37] and *Digital Rights Ireland*[38] than previously under the general principle of proportionality set out in Article 5(4) TEU in *Rechnungshof*[39].

Given the crucial importance of proportionality to data protection, we envisage issuing **a background paper** in order to further develop this guidance.

4.5. A fair balance with other public interests and fundamental rights

Ensuring that data protection becomes an integral part of EU policymaking requires not only an understanding of principles expressed in the legal framework and case law, but also a practical and creative focus on solutions to complex problems with often competing policy priorities.

---

36 *Schecke*, note 8 above, para 74.

37 *Schecke*, note 8 above para. 77 and 86. The Court held in para 81 that, when adopting measures imposing mandatory publication of certain information about beneficiaries of EU funds, the EU legislators should have taken into consideration methods of publishing such information which would be consistent with the objectives of such publication while at the same time causing less interference with those beneficiaries' right to respect for their private life in general and to protection of their personal data in particular.

38 See note 8 above.

39 *Rechnungshof*, note 21 above, para. 94. In this case, the legitimate objective of a Member State of ensuring the best use of public funds had to be balanced against the seriousness of the interference with the right of the persons concerned by salary transparency measures to respect for their private life.

The Court of Justice has recognized that EU legislation is often required to meet several public interest objectives which may sometimes be contradictory and require a fair balance to be struck between the various public interests and fundamental rights protected by the EU legal order[40]. Such rights and interests may include: the protection of life and health; the prevention and combatting of serious and organised crime, the maintenance of public order and the safeguard of security; openness, transparency and the right of access to documents; property, including intellectual property; freedom of expression; freedom to conduct a business.

We work with the EU institutions and other stakeholders to ensure that we understand the priorities and objectives behind measures which have an impact on data protection, and to assist in finding solutions which minimise conflict between these priorities. In this context, we underline that strong data protection safeguards can also enhance the effectiveness of measures intended to protect those interests.

4.6. Technology and the right to data protection

We aim to ensure that the technological aspects which are relevant for the legislative decisions are presented correctly, comprehensively and that they are up to date.

In our advice we assess the impact on data protection of technological elements of the IT systems that are created to support EU policies (e.g. in the area of freedom, justice and security or for the internal market). We also assess the impact on data protection of EU policies that are related to specific technologies (e.g. RFID, cloud computing, smart grids, eCall, body scanners) or that could trigger technical developments (e.g. initiatives in relation to trust services, cybersecurity, ecommerce, digital copyright issues, or ePrivacy). Technological elements may also play a role in other policies, e.g. open data.

[40] Case C-275/06 *Productores de Música de España (Promusicae)* v *Telefónica de España SAU*, judgment of 29 January 2008, para. 68.

In some cases, the impact of technology can only be detected and assessed by a thorough analysis. We consider that choices for technological solutions should be based on such analysis. The legislator should be aware of available technological choices and should not be left to believe that technology dictates a specific legislation without options. In particular, we aim to promote the principles of privacy by design and privacy by default.

5. Setting priorities

The EDPS faces the challenge of providing effective advice on the basis of increasingly limited resources. A selective approach based on clear criteria and rigorous planning is an indispensable condition for effective fulfilment of our advisory task.

Given the significant number of legislative proposals issued by the Commission, we establish a list of priorities[41] on a yearly basis, flagging a limited number of strategic issues, on which we wish to concentrate considerable energy. This *Inventory* is a planning and performance assessment tool. It is prepared on the basis of the annual Commission work programme, the midterm review of the program and other programming and planning tools used by the Commission, as well as bilateral contacts that we maintain with the services of the Commission. The Inventory is comprised of a list of proposals for legislation and other documents in respect of which we intend to provide advice, classified according to their priority, as well as of an explanatory document setting out our strategic approach in the area of consultation for the following year.

The inclusion of a particular planned proposal in the Inventory and the priority assigned to it are a result of an analysis based on a number of criteria. In the first place, the strategic objectives of the EDPS, as well as the Annual Management Plan are taken into account[42]. In addition, the expected impact of the proposal on the effective level of data protection in the EU is taken into account. High impact and/or intrusiveness of a planned measure, in combination with a broad scope of application would normally imply high priority. Finally, initiatives of strategic importance for EU policies and/or high political profile are likely to be subject to increased scrutiny.

---

41 Article 29, EDPS RoP.

42 Each year, an (internal) Annual Management Plan is established, translating the long term strategy of the EDPS into general and specific objectives (Article 13(1), EDPS RoP).

6. Form and timing of EDPS interventions

Without prejudice to Article 28(2) of Regulation 45/2001, a consultation on a single proposal or issue normally consists of the following steps[43]:

6.1. *Step 1*: Informal consultation[44] by the responsible service of the Commission

For our interventions to be effective, it is important that we can provide input at an early stage, ideally before the formal adoption of a proposal. Such an early consultation enables us to draw attention, in an informal manner, to aspects of the protection of personal data relevant to the proposal and – where appropriate - propose modifications of a text, without entering the political negotiations between the EU co-legislators, the European Parliament and the Council.

In consequence, in accordance with a well-established procedure[45], the EDPS is normally consulted by the Commission at an early stage of preparation of an instrument, i.e. during the inter-service consultation, and in any case before the College of Commissioners takes a final decision to adopt a legislative proposal, another measure or a policy document. In response, we provide the responsible service of the Commission with informal comments on the draft document. Such comments typically focus on technical aspects of the proposal at hand, although a more thorough analysis may be performed in cases where a proposal raises serious concerns as regards the necessity and proportionality of the proposed data processing. Informal comments provide a good indication of the issues likely to be raised in our formal opinion or comments.

6.2. *Step 2*: Formal consultation[46] by the Commission

In response to a formal consultation by the Commission following the adoption of a legislative proposal subject to the ordinary legislative procedure (Article 294 TFEU), we will, as a rule, issue a formal opinion. The same approach is taken for Commission proposals to Council and/or Parliament in specific legislative procedures. An opinion – which is normally published within three months following the adoption by the Commission – contains an analysis of the data protection aspects of a proposal which is as complete as possible.

---

43 Article 26, EDPS RoP.

44 Article 27, EDPS RoP.

45 Note of the Secretary General of the Commission to Director-Generals and Heads of Service of 8 December 2006, SEC(2006)1771.

46 Article 28, EDPS RoP.

Apart from legislative acts *sensu stricto* (i.e. regulations, directives or decisions), an opinion may also be issued on a Commission Communication, a Commission staff working document, etc. where data protection is, or should be, a core element of the draft instrument. The same reasoning applies to recommendations and opinions, as well as delegated acts (Article 290 TFEU) and implementing acts (Article 291 TFEU).

Given the need to adopt a selective approach in order to be effective in our advisory tasks, we may provide a more limited advice, in a form other than an opinion (such as formal comments or a letter) in certain cases. For other instruments, comments or letters will be the preferred option, unless there is a specific reason to adopt an opinion, e.g. because the document we comment on may have particularly serious consequences for data protection. Formal comments – normally issued within two months after the adoption of the document in question – focus on specific aspects of a proposal.

Where appropriate, we may make use of *other instruments* to convey our advice, including oral presentations, letters or press releases (not directly related to an opinion or comments). In particular, at more advanced stages of the legislative process (e.g. following the adoption of an amended proposal by the Commission, conciliation/trilogues etc.), an explanatory letter on a specific issue may be sufficient. These letters will also be published on our website.

6.3. Specific procedures[47]

6.3.1. Delegated and implementing acts (Articles 290 and 291 TFEU)

Legislative acts may provide for the adoption of delegated acts and/or implementing measures to specify in further details general provisions of that instrument. Some of these aspects may concern the processing of personal data, the modalities of which may be set out in greater details in the implementing/delegated act than in the basic act. While the basic act should normally contain a provision requiring compliance of the processing with data protection law, such a provision, however, may not sufficiently lay down the specific safeguards that are needed in view of the modalities that will be subsequently set forth in the delegated and implementing acts. We should therefore be involved, from an early stage of the process, in the drafting of delegated and implementing acts with likely data protection implications.

[47] Article 26(1), EDPS RoP.

To this end, we usually indicate in our opinion relating to the basic act that we wish to be consulted on such draft acts. In some cases, we may participate in the (expert) groups where the drafting of those acts is discussed. We should in any event be consulted informally by the Commission before the adoption of the delegated or implementing act, since it is often the only opportunity to provide input which can be taken into account.

We may also decide to react publicly after the adoption of the delegated or implementing act by the Commission, in particular to signal to the legislator whether or not the delegated or implementing act poses any threat to the privacy and data protection of individuals and if so, whether or not its necessity and proportionality has been demonstrated and appropriate safeguards provided. In doing so, we aim at guiding the legislator in making an informed decision as to its choice to accept or reject a delegated or implementing act.

6.3.2. International agreements and other bilateral and multilateral arrangements

Under Article 218 TFEU, international agreements are negotiated by the Commission and subject to Parliament's assent before they are ratified by the Council. International agreements can have an impact on the privacy and data protection of individuals even when their scope may not be about fundamental rights *per se*[48]. This is particularly the case when they contain measures providing for the exchange of personal data with recipients in third countries[49].

The EDPS should be consulted *informally* on the draft mandate given to the Commission and on the development of the negotiations before the text is initialled, as well as *formally* on the outcome of the negotiations before the Commission adopts a final proposal for a Council decision on the conclusion and signature of the agreement. Furthermore, for our contribution to be effective in successfully building in appropriate safeguards in the agreement, we should be kept informed of the progress of the negotiations, at the very least about the most salient data protection aspects. In addition, the Commission may raise, in full confidentiality, specific issues to our attention for specific advice.

---

48 E.g., privacy and data protection are core elements in the current negotiations of an EU-US umbrella agreement.

49 E.g., the Agreements on Passenger Name Records (PNR), the Terrorist Finance Tracking Programme (TFTP), drug precursors (EU-Russia) and EU agreements with third countries on customs cooperation.

A similar procedure should be followed for other bilateral and multilateral arrangements which do not formally constitute international agreements. This applies for example to the positions to be taken by the EU in joint custom cooperation committees created on the basis of bilateral agreements and providing for the exchange of information containing personal data.

Once the proposal for a Council decision with considerable impact for data protection is adopted by the Commission, we issue an opinion.

6.3.3. Communications from the Commission

The EDPS should be consulted, informally and formally, on Communications from the Commission which may have impact on privacy and personal data protection. Communications adopted by the Commission usually precede the adoption of future legislative instruments. By giving advice prior to and after the adoption of the Communication, we give expert input to help guide future legislative choices.

6.3.4. Public consultations

We may, at our own initiative, respond to public consultations launched by the European Commission or other stakeholders[50] in areas that are likely to have an impact on the privacy and data protection of individuals. Our contribution can be particularly influential in all cases where public consultations precede the adoption of legislative or legal instruments. It helps to shape any future decision-making by underlining the main data protection issues to be resolved as well as possible safeguards to remedy them.

6.3.5. Initiatives of Member States and enhanced cooperation

The Treaties still contain legislative procedures where the initiative is taken by Member States (e.g. Article 76 (b) TFEU for police and judicial cooperation). They also contain detailed provisions for enhanced cooperation (Article 20 TEU and Articles 326-334 TFEU). In these procedures, even though the Commission has a more limited role, the EDPS should play the same advisory role as elsewhere. We aim to lay down the modalities for the exercise of this role in the **Memorandum of Understanding**, as mentioned above.

[50] This may also include international organisations.

6.4. Follow-up of our interventions[51]

Our advisory role does not end with the issuance of our formal opinion (or another intervention). We continue to monitor all relevant developments and are prepared to react, where needed and appropriate, in particular in the case of opinions, in order to maximise their impact. Our involvement and the amount of resources dedicated to such follow-up depend on the priority we give to a particular proposal. However, we are prepared to consider all requests coming from the EU institutions to provide (additional) advice at later stages of the legislative process, whenever data protection issues are at stake.

In the first place, we remain available to present and discuss our advice to the co-legislators or to provide any other requested contribution. Usually, this takes the form of meetings with those directly responsible for the file in the European Parliament (the relevant Committee, the rapporteur and shadow rapporteurs) and/or the Council (the relevant Working Party and the Council Secretariat). In cases of high strategic importance (e.g. as identified in the Inventory), we will actively seek an opportunity to present our opinions in high level meetings.

In addition, we initiate regular contacts with the responsible Committee of the European Parliament and with the Secretariat-General of the Council in order to be able to follow the developments of the legislative process. Again, due to resource constraints, priority will be given to cases of high strategic importance. When, as a result of such follow-up, substantial changes are made to a legislative measure under discussion which might have potentially serious data protection implications, we may consider issuing additional advice in the form most appropriate in the circumstances.

6.5. Transparency and confidentiality

Transparency is one the core values of the EDPS[52]. We believe that acting in a transparent way, explaining what we are doing and why, in clear language that is accessible to all[53] can greatly enhance the effectiveness of the EDPS as an advisor.

---

51 Article 30, EDPS RoP.
52 Article 15(1), EDPS RoP.
53 Strategy, p. 15.

As a rule, key policy documents, guidelines, legislative opinions, formal comments, articles, letters, speeches and other deliverables are published on the EDPS website[54]. The publication in principle takes place in the working languages of the EDPS. In addition, summaries of legislative opinions are translated into all official languages of the EU and published in the *Official Journal of the European Union* (C Series)[55].

However, in order to preserve the confidentiality of the internal decision-making process of the Commission, informal comments – which are provided at the early stages of the internal decision-making process in reaction to draft documents which have not yet entered the public domain – are usually provided in confidence and are not published (although the rules on transparency and access to documents enshrined in the Treaties and in secondary legislation[56] remain fully applicable)[57]. Internal procedures also exist to ensure stricter confidentiality of documents on which we are consulted in specific cases, e.g. (draft) international agreements, sensitive documents[58], or whenever the circumstances of a particular case so require.

---

54 Article 54(1), EDPS RoP.

55 See Article 55(a), EDPS RoP.

56 Under Article 56, EDPS RoP, all documents held by the EDPS are subject to requests for public access in accordance with the principles laid down by Regulation No 1049/2001.

57 Article 27(2), EDPS RoP. In specific cases, for instance if informal comments are of general relevance, may provide useful guidance to other stakeholders or have an impact in other areas of EDPS activities, we may decide to publish our input in an appropriate form, following a consultation with the Commission.

58 See Article 9 of Regulation No 1049/2001 of the European Parliament and of the Council of 10 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, p. 43.

6.6. Other interventions

While *position papers* are normally adopted in the context of the EDPS' supervisory tasks, we may also issue a *background paper*[59] to give our views on how to come to a balanced and proportionate approach to data protection in a particular field where there is a need for a preliminary or further developed analysis. Finally, a *policy paper* may be adopted to clarify the way in which the EDPS intends to exercise his tasks and powers, such as the consultative role with respect to proposals for new legislation[60]. These instruments enhance the effectiveness of the advisory work of the EDPS and seem particularly well suited for the promotion of a general data protection culture within the EU Institutions and bodies.

In addition, we endeavour to identify strategic policy themes and act more proactively, by providing advice *ex officio*, without a formal legislative proposal, often in the form of an *opinion*[61] or a *preliminary opinion*[62].

---

59 E.g. "Public access to documents containing personal data after the Bavarian Lager ruling", 24 March 2011, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf

60 E.g. the 2005 Policy Paper, note 3 above.

61 E.g. Opinion on the Commission Communication on "Unleashing the potential of Cloud Computing in Europe", 16 November 2012, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

62 E.g. Preliminary Opinion "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

The EU approach to data protection is guided by the rulings of the Court of Justice of the European Union interpreting the provisions of the applicable legal framework, including Directive 96/45/EC and Regulation 45/2001. We aim to play a pro-active role in this area by implementing Article 47(1)(i) of Regulation 45/2001, which grants the EDPS the power to intervene in actions brought before the Court of Justice[63]. In this context, we strive to provide impartial, expert advice on matters falling within our competence in a manner similar to the *amicus curiae* ("friend of the court") briefs known to some jurisdictions. Our interventions should therefore be seen as part of our advisory role in the broadest sense, i.e. encompassing also the provision of data protection expertise during legal proceedings before the Court[64].

Finally, we use a number of other means to raise awareness of data protection issues, including publications on our website and the organisation of workshops, meetings and seminars.

7. Cooperation

The independent supervisory authorities monitoring the application of data protection laws in EU Member States collaborate in the framework of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (also known as the "Article 29 Working Party" or the "WP29") established under Article 29 of Directive 95/46/EC. The WP29 advises the Commission on the level of protection in third countries, on any proposed amendments of the Directive 95/46/EC, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data *and on any other proposed Community measure affecting such rights and freedoms*[65] (emphasis added).

---

63 See also Article 41, EDPS RoP.

64 Information on EDPS interventions before the Court can be found at: https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Court.

65 Article 30(1)(c) of Directive 95/46/EC.

As a member of the WP29[66], we contribute to the work programme of the Group and we participate in the plenary and subgroup meetings (including drafting and/or contributing to opinions and other texts), as appropriate to ensure consistency and provide the unique EU perspective. We also ensure regular coordination, in particular with the Chair of the WP29, in order to develop synergies.

In January 2012, the Commission adopted the proposals for a General Data Protection Regulation ("GDPR") and for a Directive in the field of law enforcement. One of the key elements of these proposals was the creation of a European Data Protection Board ("EDPB") that would replace the WP29. Under the so-called consistency mechanism, the EDPB would become the central instance in the enforcement of data protection law in cases with an EU wide dimension.

Under the Commission proposal, the Secretariat of the EDPB (including analytical, administrative and logistical support) will be provided by the EDPS[67]. This arrangement would allow the EDPB to exercise its functions with complete independence and strong legal powers, while at the same time taking advantage of synergies and cost savings resulting from secretarial support of an existing structure.

Finally, we work with other EU bodies which advise EU institutions and Member States on certain aspects related to fundamental rights (such as the Fundamental Rights Agency FRA) or to information security (the European Network and Information Security Agency ENISA), and we contribute to activities in a number of international organisations such as the Council of Europe. We follow and actively contribute as observer to the discussions of the Consultative Committee of Convention 108, of its Bureau and of the Ad-Hoc Committee on Data Protection

---

66 Article 46(g) of Regulation 45/2001.
67 Article 71(2) of the proposed GDPR.