Guidelines on the Rights of Individuals with regard to the Processing of Personal Data

INTRODUCTION 4

SCOPE AND STRUCTURE OF THE GUIDELINES 6
Scope: what is in and what is not? 6
What are the data subject's rights? 7
"Rights of the Data subject" under Section 5 of the Regulation 7
Which exceptions apply? 7

Part 1: The different rights of the data subject 9
1. Right to access, Article 13 of the Regulation 11
a) General remarks 11
b) The right of access in the light of specific procedures 13
Selection procedures: Access at least to aggregated results 13
Staff evaluation procedures 14
Administrative inquiries and disciplinary procedures 14
Medical files/health data 15
Grant and procurement award procedures 16
c) Article 13 of the Regulation: "step by step" 16
2. Rectification, Article 14 of the Regulation 18
a) General remarks 18
b) The right to rectify in the light of specific procedures 19
Selection and recruitment of staff 19
Evaluation procedures 19
Medical data 20
Administrative inquiries and disciplinary procedures 20
Blacklisting / asset freezing 20
3. Blocking, Article 15 of the Regulation 21
4. Erasure, Article 16 of the Regulation 22
Administrative inquiries and disciplinary procedures 23
Blacklisting / asset freezing 23
5. Notification to third parties, Article 17 of the Regulation 23
6. The right to object, Article 18 of the Regulation 24
7. Special rights in case of automated individual decisions, Article 19 of the Regulation 25

Part 2: Exceptions and restrictions 26
Article 20(1)(a) of the Regulation: "...prevention, investigation, detection and prosecution of criminal offences" 27
Article 20(1)(b) of the Regulation: "...an important economic or financial interest..." 28
Article 20(1)(c) of the Regulation: "... protection of the data subject or of the rights and freedoms of others" 29
Selection & recruitment procedures 29
Medical files 31
Procurement 31
Administrative inquiries and disciplinary procedures 32
Harassment 33
Access to documents under Regulation (EC) No. 1049/2001 33
Article 20(1)(d) of the Regulation: "...the national security, public security or defence of the Member States" 33
Article 20(2) of the Regulation 34
Article 20(3)-(5) of the Regulation 34

Part 3: What the EDPS does to protect data subjects' rights 36

INTRODUCTION

1. These guidelines ("Guidelines") are issued by the European Data Protection Supervisor (the "EDPS") in the exercise of the powers conferred on him under Articles 41(2) and 46(d) of Regulation 45/2001 on the protection of personal data by European Union institutions and bodies ("the Regulation")[1].

2. The Guidelines provide guidance to the European Union institutions and bodies ("EU institutions") as to how the EDPS interprets the provisions in Sections 5 ("Rights of the Data Subject") and 6 ("Exemptions and Restrictions") of the Regulation.

3. The Guidelines are addressed to all services within the EU institutions which process personal data. Additionally, they aim to guide the EU institutions' data protection officers ("DPOs"), staff representatives, data subjects and the general public.

4. The Guidelines implement the strategic objective of promoting a 'data protection culture' within the EU institutions and bodies so that they are aware of their obligations and accountable for compliance with data protection requirements. They specifically implement the first action point under the EDPS Strategy 2013-2014 to provide guidance and training for data controllers, DPOs and Data Protection Coordinators ("DPCs").

5. The content of these Guidelines is based on the *acquis* of EDPS positions in the area of data subjects' rights developed in Opinions on data processing operations by EU institutions. For a list of all cases cited in these Guidelines, please see the Annex.

6. The prior-check or consultation Opinions of the EDPS on data subjects' rights as well as thematic guidelines published so far, constitute the main building block of these Guidelines. That said, following the Guidelines is often the most efficient way to ensure compliance with the Regulation. The Guidelines present in a clear way the outcome of the EDPS positions and recommendations regarding the relevant principles of the Regulation, provide information about existing best practices and underline other particular issues.

7. The EDPS position is without prejudice to the case law of the Court of Justice of the European Union (CJEU), and to the interpretation that the European Courts may give to those provisions in the future.

8. **What's next?** In January 2012, the Commission made proposals for a thorough revision of the rules on data protection which currently apply to

[1] Regulation (EC) 45/2001 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, 12.01.2001, p. 1.

the Member States (e.g. Directive 95/46/EC). These proposals also include some enhanced rights, such as the right of erasure or "right to be forgotten" and the right to "data portability", that seem to be particularly useful in the online environment. The Regulation will be brought in line with this important reform.

SCOPE AND STRUCTURE OF THE GUIDELINES

Scope: what is in and what is not?

These Guidelines cover rights attributed to **data subjects** by the Regulation. The data subject is the person whose personal data are collected, held or otherwise processed[2]. The range of individuals entitled to these rights is quite broad, as explained in Recital 7 of the Regulation: "*The persons to be protected are those whose personal data are processed by Community institutions or bodies in any context whatsoever, for example because they are employed by those institutions or bodies*".
Recital 5 of the Regulation stipulates that: "*A Regulation is necessary to provide the individual with legally enforceable rights*...". The present Guidelines cover these rights with the following exceptions:

- Data subjects are safeguarded by a **general right**, which is that the EU institutions must process their personal data fairly and lawfully, and only for legitimate purposes (Articles 4 to 6 of the Regulation). This general right is not directly covered by the present Guidelines.
- This general right is complemented by a number of specific rights of the data subject, including the **right to be informed** stipulated in Section 4 of the Regulation. This obliges the controller to provide the data subjects with information such as the identity of the controller[3], the purpose of the processing, the recipients of the data and the rights of the data subjects. The data subject is also entitled to be informed before his or her personal data are disclosed for the first time to third parties. The data subject has the right to object to such disclosure. The present Guidelines do not discuss the right to be informed, they are built on the assumption that data subjects have been informed of their rights under the Regulation. Please see below (p. 8), where we briefly address the issue of informing data subjects.
- Although data subjects' rights constitute rules of law conferring rights on individuals, these Guidelines do not cover issues of **non-contractual liability** for the breach of such rules under Article 340 TFEU[4].

---

[2] See http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/74. For further definitions, see Glossary annexed to these Guidelines.

[3] Article 2(d) of the Regulation stipulates that "'controller' shall mean the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Community act, the controller or the specific criteria for its nomination may be designated by such Community act". The concepts of "Community institutions and bodies" and "Community law" cannot be used any longer after the entry into force of the Lisbon Treaty on 1st December 2009. Article 3 of Regulation 45/2001 must therefore be read in light of the Lisbon Treaty, to refer to EU institutions and EU law .

[4] Treaty on the Functioning of the European Union; see e.g. case T-259/03, where the European Anti-Fraud Office (OLAF) divulged personal information in the context of an inquiry concerning a Member of the Court of Auditors and the Court found that in the particular case,

What are the data subject's rights?[5]

"Rights of the Data Subject" under Section 5 of the Regulation

Section 5 of the Regulation entitled "Rights of the Data Subject" contains a set of specific data subject rights. Except in certain determined cases, data subjects can obtain from the controller free of charge:

- **access** to their own data (Article 13 of the Regulation). Data subjects have the right to receive from an EU institution (at any time within three months from the receipt of the request) information as to whether or not personal data relating to them are being processed, as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed as well as to communication in an intelligible form of the personal data undergoing processing;
- the **rectification** without delay of inaccurate or incomplete data related to them (Article 14 of the Regulation);
- the **blocking** of their data under certain circumstances (e.g. when the accuracy of the data is contested) (Article 15 of the Regulation);
- the **erasure** of their data for instance if their use is unlawful (e.g. processing of sensitive data) (Article 16 of the Regulation);
- the **notification to a third party** to whom the data have been disclosed of any deletion, rectification or blocking of their data (Article 17 of the Regulation);
- On compelling legitimate grounds, data subjects can **object** at any time to the processing of data relating to them (Article 18 of the Regulation);
- Special rights exist in case of automated individual decisions (Article 19 of the Regulation)

Part 1 of these Guidelines follows this structure.

Which exceptions apply?

Under **Article 20** (**Section 6) of the Regulation** (entitled "Exemptions and Restrictions"), data subjects' rights can be restricted, but they cannot be denied. This limitation can take place in specific cases, for a determined period of time and only if necessary, to safeguard:

- the prevention, investigation, detection and prosecution of criminal offences (as well as of disciplinary proceedings and administrative enquiries). This could apply, for example, to investigations carried out

---

"*il convient de présumer, en l'espèce, que la fuite constatée ci-dessus résulte d'une violation de l'article 8, paragraphe 3, du règlement n° 1073/1999 commise par le directeur de l'OLAF dans l'exercice de ses fonctions, au sens de l'article 288 CE*" ("*It is appropriate to presume, in the case at hand, that the leak established above results from a violation of Article 8, paragraph 3 of Regulation No 1073/1999 committed by the Director of the OLAF in the exercise of his duties, in the sense of Article 288 EC*" - inofficial translation).

[5] See also http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA5.

by the European Anti-fraud Office (OLAF) or the Commission's Investigation and Disciplinary Office (IDOC);

- an important economic or financial interest of a Member State or of the European Union;
- the protection of the data subject or of the rights and freedoms of others;
- the national security, public security or defence of the Member States.

Part 2 of these Guidelines contains respective guidance.

The issue of informing data subjects

As noted above, for the purpose of these Guidelines, we assume that data subjects have been informed of their rights under the Regulation. Articles 11 and 12 of the Regulation list the information which must to be supplied to the data subject depending on whether the data have been obtained from the data subject himself/herself (Article 11) or not (Article 12).

Providing individuals with the required elements of information not only puts them in the position of effectively exercising their data subject rights, but also contributes to ensuring data quality in the sense of Article 4 of the Regulation (e.g. "fair processing" and accuracy of the personal data). Where consent is used as a legal basis, Article 2(h) of the Regulation highlights the importance of informing the individual by referring to "any freely given specific and *informed* indication" of the data subject's wishes signifying his or her agreement to personal data relating to him or her being processed (emphasis added).

The EDPS has addressed the issue of providing information to data subjects on several occasions[6]. These cases illustrate that the information can be provided in a number of formats (most often via webpages or paper handouts) and that the exact scope of the information (e.g. on the purposes of the processing operation, the legal basis or the applicable time limits) will vary from case to case.

What does the EDPS do to protect data subjects' rights?

Part 3 of these Guidelines gives a short overview of what we do to protect data subjects' rights.

[6] See e.g. case 2011-0752 or the EDPS Video-surveillance Guidelines, p.44.

Part 1: The different rights of the data subject

The "Rights of the Data subject" listed in Section 5 of the Regulation display certain common features:

- The preamble states that the Regulation is necessary to provide the data subject with legally **enforceable rights** and to specify the data processing obligations of the controllers (see Recital 5). The controller -regularly the EU institution responsible for the data processing operation- is thus subject to a positive **obligation** to act in order to allow individuals to exercise their right.

> In a notification regarding the processing of personal data of temporary staff, the rights of access and rectification were not attributed to the data subjects concerned, but limited to their *employment agency*[7]. In our recommendations, the EDPS noted the obligation of the EU body to ensure that the temporary staff themselves (instead of their employment agency) can effectively exercise their rights under Articles 13 and 14 of the Regulation.

- This also means that the **controller must ensure** that the data subject can make **effective use** of these rights. The mere mention of these rights is insufficient[8]; the data subject is entitled to receive adequate information as to how these rights are guaranteed and which limitations might apply.

> In a case regarding a database containing evaluation results, the EDPS noted that in order to ensure the accuracy and completeness of the data, there was an informal process by which data subjects could contest the assessment made by an expert group[9]. It was then up to this group to re-evaluate the pertinence of the arguments and remove any mistakes from the database. The EDPS recommended that the EU institution clearly inform the data subjects of their rights to contest the accuracy of the data, and to rectify them.

- Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (see **Article 24(8)** of the Regulation) usually contain a chapter concerning the **internal procedure** on how the data subjects can exercise their rights[10].

- The controller must further ensure that data subjects can effectively exercise their rights **within reasonable time limits**:
  - "Without delay" for the right to rectification;
  - Promptly, for the rights to blocking and erasure;

---

[7] See case 2010-0796.

[8] See Opinion in case 2011-0806: "*La simple citation de ces droits ne suffit pas, car il est nécessaire d'expliquer adéquatement les moyens de les garantir ainsi que les limitations de ces droits qui sont applicables dans le cadre des traitements en question*".

[9] See case 2010-0869.

[10] See respective recommendation in Opinion in case 2011-0101: "*The EDPS invites the ESRB to determine its modalities for granting these rights, when adopting its own implementing rules under Article 24(8) of the Regulation and submit a copy before adoption to the EDPS for consultation under Article 28(1) of the Regulation*".

- “Within 3 months” for the right to access.

1. Right of access, Article 13 of the Regulation

a) General remarks

Data subjects have the right to access their own personal data (Article 13 of the Regulation). This means that they are entitled to receive from an EU institution at any time within three months from the receipt of the request and free of charge:

- confirmation as to whether or not data related to them are being processed;
- information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
- communication in an intelligible form of the data undergoing processing and of any available information as to their source;
- knowledge of the logic involved in any automated decision process concerning them.

The right of access is specifically granted by Article 8 of the European Charter of Fundamental Rights. It enables data subjects to check the quality of their personal data and the lawfulness of the processing[11]. In the context of investigations, this coincides largely with the right of defence.

The right of access is also a precondition for the exercise of other rights, such as the rights of rectification, blocking and erasure[12]. The right of access and the right of rectification are directly connected to the data quality principle. However, the data subject has a right of access to his or her data even where the data are accurate and complete; the EDPS has highlighted that a limitation to cases where data are inaccurate or incomplete only applies to the right of *rectification*, not to the right of *access*[13].

The right to access thus helps data subjects:

- to understand which data are processed about them;
- to verify the quality of their personal data;
- to verify the lawfulness of the processing; and
- to exercise their other data protection rights.

Access shall therefore be **granted to the fullest extent** unless an exemption under Article 20(1) of the Regulation applies (see Part 2 of these Guidelines).

---

[11] See Recital (41) Directive 95/46/EC: "*Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing*" (case 2009-0550).

[12] CJEU, C-553/07, *Rotterdam v. Rijkeboer*: §51: "*That right of access is necessary to enable the data subject to exercise the rights set out in Article 12(b) and (c) of the Directive, that is to say, where the processing of his data does not comply with the provisions of the Directive, the right to have the controller rectify, erase or block his data, (paragraph (b)), or notify third parties to whom the data have been disclosed of that rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort (paragraph (c))*".

[13] See case 2011-0483.

In the light of the narrow interpretation given to those exceptions and their applicability on a case-by-case basis, access **must not be restricted more broadly than necessary**.

The right of access is the right of data subjects to be informed about any information relating to them that is processed by the controller, whether the data were provided by themselves or not[14]. As a matter of principle, this right has to be interpreted in relation to the concept of personal data.

Personal data pursuant to Article 2(a) of the Regulation shall mean "*any information relating to an identified or identifiable natural person*". Indeed, the Regulation has adopted a **broad concept of personal data**, and the Article 29 Data Protection Working Party has also followed a wide interpretation of this concept[15]. In the light of this broad concept, personal data under the Regulation clearly refers to **more than just the name of a particular data subject**. The Working Party 29 has clarified that information is "*relating to*" a data subject in the sense of Article 2(a) of the Regulation, if it refers to the identity, characteristics or behaviour of an individual (*content element*), or if information is used to determine or influence the way in which that person is treated or evaluated (*purpose element*) or if the use of the data is likely to have an impact on the data subject's rights and interests (*result element*).

With regard to allegations of maladministration a complainant raises against an institution which contain also references to a **qualified third party** and his/her behaviour, the EDPS' view is that such allegations are not only the personal data of the person raising the allegations, but also of the person who is accused or involved in the alleged wrongdoing. For instance, in cases concerning investigations by the European Anti-Fraud Office, the EDPS found that "*statements made regarding the events under investigation [...] about the person*" as well as "*evidence mentioning the person and notes regarding the relation of the person to the events under investiga*tion" can be considered personal data of that qualified third party[16].

However, the fact that a person's name is mentioned in a document does not necessarily mean that all information in that document should be considered as data "relating to" that person. This depends on a further analysis of that information in the light of the above mentioned criteria.

The EDPS has clarified that where according to a particular retention policy certain personal data need to be retained, it is possible to erase these before the end of the established retention period where they have been *unlawfully* processed[17]. Reasoning *e contrario* personal data which have been *lawfully*

[14] See case 2011-0483).

[15] Opinion 4/2007 on the concept of personal data, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf. The **Article 29 Data Protection Working Party** was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the **protection of individuals** with regard to the processing of personal data and on the **free movement** of such data.

[16] See case 2005-418.

[17] See case 2009-0550. This is because under such circumstances, erasure represents a measure adopted in order to ensure compliance with the Regulation, see below Section 4.

processed should be available in principle until the end of the applicable **retention period** in the case of an access request.

Access can be obtained directly by the data subject ("direct access") or, under certain circumstances, via an intermediary ("**indirect access**"). Where the intermediary is a public authority, in the context of these Guidelines, it will be the EDPS as the data protection supervisory authority of the EU institutions (see also below on Article 20(4) of the Regulation).

Furthermore, the right of access is also applicable when a data subject requests **access to the file of a third party**, where information relating to him or her would be involved. This might be the case for **whistleblowers, informants or witnesses** asking for access to data relating to them in an investigation conducted against another individual.

A clear distinction should be made between the right of public access to documents under **Regulation (EC) No. 1049/2001** and the right of access of data subjects to their own personal data under Article 13 of the Regulation. Requests from data subjects for *their own personal data* should always be treated under the second category (i.e. the right of access under Article 13 of the Regulation). For further guidance on the relationship between the two Regulations in the light of the case law of the Court of Justice, please refer to the EDPS Background Paper "*Public access to documents containing personal data after the Bavarian Lager ruling*"[18].

b) The right of access in the light of specific procedures

Selection procedures: Access at least to aggregated results

Regarding selection procedures (pre-selection tests, interviews and written examinations), data subjects should in principle be given access to their evaluation results regarding **all stages of the procedure**. Even where an exception under Article 20(1)(c) of the Regulation in line with Article 6 of the Annex III to the Staff Regulations might apply (see below, Part 2), data subjects should nonetheless be provided with **aggregated results**.

Aggregated results means that no information regarding the *individual marks* or assessments attributed *by each individual* evaluator/jury member involved is given[19]. However, the average mark resulting from the *aggregation of the individual marks*/assessments by *all* evaluators/jury members should be disclosed in a transparent manner.

In a recruitment case, the EDPS established that the EU body concerned "*should be in a position to give a detailed breakdown of the mark given for the oral test, i.e. to give the mark for each section on which the applicant was assessed at the oral, without that interfering in any way with the principle of the secrecy of selection board proceedings, as set out in Article 6 of Annex III to the Staff Regulations, since the*

[18] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.
[19] See cases 2004-0236, 2011-0101 and 2007-0422.

marks given would be overall averages. There is certainly no question of revealing marks given by individual members of the board or any information on comparison with other applicants"[20] (emphasis added).

In another case, the EDPS recommended that the agency in question should provide access, upon request, to the minutes of the selection boards, but pointed out that "*if necessary to safeguard the confidentiality of the deliberations and decision-making of the selection board, certain information may be deleted from the minutes. For example, if opinions varied about a candidate's performance at the interview, it is not always necessary to indicate which selection committee member favoured and which did not favour the applicant*"[21].

In two cases regarding the selection of members of Scientific Committees, the EDPS concluded that candidates should be able to have access to their entire files, including inter alia the assessment form concerning them drafted by the various evaluators involved during all stages of the selection procedure[22].

Staff evaluation procedures

As noted in the Guidelines on staff evaluation (p. 7)[23], in the context of evaluation procedures, data subjects are in principle provided with a copy of their reports and are invited to make comments on them, as foreseen in Articles 34 and 43 of the Staff Regulations, as well as Articles 14 and 84 Conditions of Employment of Other Servants (CEOS). Under Article 26 of the Staff Regulations, as well as Articles 11(1) and 81 of the CEOS, data subjects can also obtain access to all the documents in their personal file even after leaving the service.

Administrative inquiries and disciplinary procedures

In principle, the EDPS notes that access to personal data is essential not only for data subjects' rights under the Regulation, but also to the right of defence.

As highlighted by the EDPS Guidelines on administrative inquiries and disciplinary procedures (p. 8)[24], the EDPS considers that the wording of Article 13(1) of Annex IX of the Staff Regulations deserves special attention: "... *the official concerned shall have the right to obtain his complete personal file...*" The reference to the *personal file* is misleading since it is beyond doubt that the purpose of this rule is to grant the data subject full access to his or her personal data within documents which are, or may be of importance with regard to proper defence during a disciplinary procedure. These documents are included in the *'disciplinary file'*. According to the correct interpretation of the paragraph in question, the official concerned shall have *de facto* the right to obtain his complete *"personal"* (i.e. on him/her) disciplinary file and obtain the communication in an intelligible form of his or her personal data contained in all documents relevant to the proceedings, including exonerating evidence.

[20] See case 2004-0236.
[21] See case 2007-0422.
[22] See cases 2011-0101 and 2010-0980.
[23] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/11-07-15_Evaluation_Guidelines_EN.pdf.
[24] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-04-23_Guidelines_inquiries_EN.pdf.

In this context, it is necessary to emphasise that a disciplinary procedure in progress does not affect the data subject's right of access to his or her personal file.

- In the course of a disciplinary procedure, data subjects are thus in principle granted full access to their personal file without restriction. As highlighted in the EDPS Guidelines on administrative inquiries and disciplinary procedures (p. 8), data subjects are granted full access to the documents in their disciplinary file, as well as to the copies of the final decisions stored in their personal file[25].

- Restrictions may apply in the frame of administrative inquiries or harassment procedures. For example, data subjects will normally be granted access to the conclusions of the investigation report, which contain relevant information concerning them. However, access will probably be refused to the whole case file, and in particular to testimonies from complainants or witnesses, because this access could undermine the rights and freedom of others (Article 20(1)(c) of the Regulation, see below). At any rate, such limitations should be clearly spelled out in the procedures and in the respective data protection notice.

In case 2011-0806, the EDPS underlined that " *in the course of an administrative inquiry or disciplinary proceedings, data subjects must have access without constraint to the documents contained in their disciplinary file and also to copies of final decisions placed in their personal file. However, such access may be restricted if application of the restrictions defined in Article 20 of the Regulation is justified. The EDPS recommends that this principle be clearly set out in the general provisions and also in the information notice*".

Medical files / health data

Regarding medical files, as pointed out in the EDPS Guidelines on health data (p. 14/15)[26], data subjects should not be requested to specify the purpose of their request for access. By virtue of Article 26(a) of the Staff Regulations, staff members have the right to acquaint themselves with their medical files, in accordance with arrangements laid down by the institutions. In this respect the EDPS also calls attention to the Conclusions 221/04 of 19 February 2004 of the "*Collège des Chefs d'administration*", which aim at harmonizing certain aspects of access provisions across the institutions and bodies of the European Union and emphasizes that access to health data must be provided to the maximum extent possible.

Where psychological or psychiatric data is concerned, direct access to this information may present a risk to the data subjects in question. The EDPS has stated

[25] See also case 2010-0752.
[26] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_EN.pdf.

that in such situations, the EU administration should ensure that data subjects have indirect access to their personal data following a case by case assessment[27] (see below p. 34). This is based on Article 20(1)(c) of the Regulation.

Grant and procurement award procedures

The EDPS has highlighted that all data subjects, including those participating in calls for expression of interest, should be given access to their evaluation results following the respective selection procedure, unless a restriction provided for by Article 20(1) of the Regulation applies[28].

c) Article 13 of the Regulation: "step by step"

"The data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge from the controller:..".

- **Without constraint**: As expressly noted by the EDPS Guidelines on staff recruitment (p. 7/8), but not limited to instances of staff recruitment, a request for access may be submitted in any written format. For example, requests can be made by e-mail or by filling in an access request form, although the use of the latter cannot be made mandatory.

- Regarding CCTV footage, the EDPS Guidelines on Video-surveillance (pp. 46/47)[29] note that the provision of access (and more detailed information) **free of charge** should also be a default policy in terms of video-surveillance recordings. However, the default policy may be changed by a reasoned decision if the number of access requests significantly increases, in order to discourage vexatious or frivolous requests. In this case one can start charging a *reasonable amount* for the provision of actual copies or viewings of the recordings, to help cover the costs incurred by the provision of access. The charge must not be excessive and must not serve to discourage legitimate access requests. A charge for access provision must be noted in the video-surveillance policy.

- Access to the data must be provided **within a reasonable time** from the date of the request (i.e. normally within three months maximum). As regards CCTV footage, the EDPS Guidelines on Video-surveillance (p. 46/47) note that, whenever possible, access should be given within 15 calendar days. If this is not possible, another meaningful response (not merely an acknowledgement of receipt) should be given within 15 calendar days. Irrespective of the complexity of the case, granting access (or providing a final, meaningful response rejecting the access) must not be delayed beyond the three months maximum period

[27] See case 2010-0071.
[28] See case 2011-0103.
[29] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf.

provided for in the Regulation. In most cases, access should be granted much earlier.

"... (a) confirmation as to whether or not data related to him or her are being processed ...".

Purpose: Such confirmation should allow the data subject to exercise his or her different data protection rights, e.g. letting the data subject know whether he/she is subject to an investigation. Such an investigation could be an internal one[30] or an inquiry conducted by OLAF[31].

Format: The way in which the "confirmation" should be provided depends, to a certain extent, on the nature and characteristics of the data and the processing activity involved[32]. It also depends on whether a particular way of providing the confirmation allows the data subject to exercise his or her different data protection rights or not[33]. For example, a request to receive a list of cases where the data subject's personal data appears can be considered a means to enable the verification by the data subject of his or her personal data and does not appear, *prima facie*, to be a disproportionate request[34]. The EDPS has further accepted a blanket request such as "*all data currently held by (a particular EU body) about me*"[35]. However, the EDPS has also stated that whilst the level of detail has to enable the data subject to evaluate the accuracy of the data and the lawfulness of the processing, **the burden of the task for the controller has to be kept in mind**[36].

"... (c) communication in an intelligible form of the data undergoing processing and of any available information as to their source;...".

Format: The right of access is usually granted by providing paper or electronic copies of the data subject's personal data. Sometimes the format of the data to be transmitted must be adapted to the data subject (such as in the case of a blind person who needs electronic copies[37]). Providing access to the file on the premises of the controller also qualifies as a legitimate solution, provided that it leads to a "*communication in an intelligible form of the data undergoing processing and of any available information as to their source*" pursuant to Article 13(c) of the Regulation, which also gives individuals the possibility of exercising their other data subject rights[38].

[30] See complaint 2008-0257.
[31] See e.g. case 2009-0550.
[32] See case 2009-0550.
[33] See point 57, Judgement of the CJEU in C-553/07, Rotterdam v. Rijkeboer.
[34] See C-553/07, *"51. That right of access is necessary to enable the data subject to exercise the rights set out in Article 12(b) and (c) of the Directive, that is to say, where the processing of his data does not comply with the provisions of the Directive, the right to have the controller rectify, erase or block his data, (paragraph (b)), or notify third parties to whom the data have been disclosed of that rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort (paragraph (c))".*
[35] See case 2012-0586.
[36] See case 2009-0550.
[37] See case 2009-0151.
[38] See case 2012-0841.

Individuals must be granted access to their data **in an intelligible form**. It should be recalled that the right of access is meant to enable data subjects to control the quality of their personal data and the lawfulness of the processing. This means that in certain cases, extra information must be provided to the data subject to allow his understanding. As noted in the EDPS Guidelines on health data (p. 15), this may imply, for example, that the medical practitioner of the institution concerned must interpret the data (such as medical codes or the results of a blood analysis) and/or make the data decipherable.

"...d) knowledge of the logic involved in any automated decision process concerning him or her ...".

This refers to automated individual decisions under Article 19 of the Regulation. The data subject needs to have knowledge of the logic involved in an automated decision process to understand the processing operation.

2. Rectification, Article 14 of the Regulation

"The data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data".

a) General remarks

Like the right to access, the right to **rectification** under Article 14 of the Regulation is a right specifically granted by Article 8 of the European Charter of Fundamental Rights. The EDPS considers that on certain occasions, the right of rectifying data is exercised jointly with the right of blocking the data, e.g. when the data subject disputes their accuracy (Article 15 of the Regulation, see below). In this context, the EDPS has criticised systems that do not provide for the possibility to have a set of *individual* personal data rectified without blocking the *whole system* (see the case of Sysper2[39]).

The right of rectification **only applies to objective and factual data[40]**, not to subjective statements (which, by definition, cannot be factually wrong). The EDPS has noted that in the context of a "conduct evaluation" it is difficult to determine whether personal data are *"inaccurate"* or not[41]. However, data subjects are permitted to complement existing data with a second opinion or counter expertise in such situations, e.g. as regards decisions made during an appeal procedure in disciplinary cases[42], or comments on an annual performance appraisal.

[39] See case 2006-0436.
[40] E.g. identification data, which can be rectified at any time during a selection procedure (case 2007-566) or identification data linked to an administration management system when making use of a flexitime system based on RFID technologies.
[41] Guidelines concerning the processing of personal data in administrative inquiries and disciplinary proceedings by European institutions and bodies, p. 4.
[42] See e.g. case 2011-0806.

In the context of an EU body's informal procedure for the prevention of psychological and sexual harassment[43]), the EDPS advocated that a distinction be made between objective/hard data and subjective/soft data when granting the right to rectification. Whilst inaccurate "hard data" should be rectified following Article 14 of the Regulation, inaccurate "soft data" can only relate to the fact that specific statements have been made by the data subject (which then again is a *factual* statement which can be rectified). The EDPS additionally noted that in the case of soft data, to ensure the completeness of a file, data subjects may also ask to add their opinion to it.

b) The right to rectify in the light of specific procedures

Selection and recruitment of staff

The EDPS Guidelines on staff recruitment (p. 8)[44] point out that after the closing date of submitting applications, the right of rectification is limited to data relating to the admissibility criteria. The EDPS considers this limitation necessary for the fairness of the selection procedure, and justified in terms of Article 20(1)(c) of the Regulation (see below). It is however important that all applicants are informed about the scope of this restriction before the beginning of the processing operation.

In the Anti-harassment Guidelines (p. 11), the EDPS referred to the selection of confidential counsellors and the right of rectification of the data processed by the panel during its selection. In this context, the EDPS noted that it is obvious that only objective and factual data may be rectified, and not appreciations by the members of the selection panel. This is because such appreciations are the result of a subjective assessment and as such inherent to the selection procedure.

Evaluation procedures

The subjective appraisal made by a superior in an evaluation report cannot be rectified, whereas the name, the grade or any other factual data can. Regarding subjective data, the requirement of accuracy cannot appertain to the accuracy of a particular statement[45] (*subjective* data, i.e. not accurate or inaccurate as such), but merely to the fact that a particular statement has been made. The EDPS Guidelines on staff evaluation (p. 7) note that evaluation data can be rectified within the respective *appeal* procedures. In any case, it should be ensured that the revised reports are added to the personal file.

Regarding a database used to process feedback for further development of managers, the EDPS acknowledged that given the subjectivity involved in the feedback exercise, as well as its purpose, the right of rectification is rather limited[46].

[43] See case 2012-0598.
[44] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/08-10-10_Guidelines_staff_recruitment_EN.pdf.
[45] Even where an assessment is *based on incorrect facts*, the requirement of accuracy cannot appertain directly to the accuracy of that particular assessment (it might still be accurate for other reasons), but only to the underlying facts.
[46] See case 2011-0511.

Medical data

As noted in the EDPS Guidelines on health data (p. 16), the right to rectify inaccurate or incomplete data is somewhat limited as regards certain medical data, to the extent that the accuracy or completeness of medical data is difficult to evaluate. However, data subjects should have the possibility to complement existing data with a second medical opinion.

Regarding the possibility to rectify the medical file, the EDPS has stated that "*With regard to the right of rectification, the (institution) should explain to data subjects, for example in the information note, that their right of rectification implies not only to the rectification of administrative errors in their medical file but also their right to supplement it by adding second medical opinions*..."[47].

Administrative inquiries and disciplinary procedures

The EDPS has acknowledged (see Guidelines on administrative inquiries and disciplinary procedures, pp. 9/10) that in the context of a *conduct* evaluation, it can be difficult to determine whether personal data are *"inaccurate"* or not. Data subjects should therefore be allowed to add their comments to their disciplinary file, to ensure completeness. For the same reason, decisions made during a recourse or appeal procedure should also be included in the disciplinary file as well as in the personal file. Where such a decision has been successfully challenged in a recourse or appeal procedure, it should be replaced or removed accordingly.

The EDPS has pointed out that data subjects should be informed about their right to add their comments, to include a recourse or appeal decision in their files, and, where applicable, to ask that the decision is replaced or removed from the file[48].

Blacklisting / asset freezing

Given the sensitivity of the personal data involved in the case of blacklisting mechanisms (e.g. Early Warning System[49]), the right of rectification is of a key importance in order to guarantee the quality of the data used, which may be connected to the right of defence[50].

As regards asset freezing, the EDPS has recommended the establishment of clear, transparent and homogeneous rules to allow data subjects to exercise their rights of access and/or rectification to all of their personal data in relation to all regulations covered by the notification[51]. He has further noted the need for a rule according to which, where a listing has been declared originally unlawful on the basis of the review procedures, a corrigendum in the Official Journal is published mandatorily (see also below, Section 4 "Erasure").

[47] See case 2011-0655.
[48] See cases 2010-0752 and 2011-0806.
[49] The purpose of the EWS is to ensure within and between EU institutions the circulation of restricted information concerning third parties who could represent a threat to the EU's financial interests and reputation.
[50] See case 2008-0374.
[51] See case 2010-0426.

3. Blocking, Article 15 of the Regulation

"The data subject shall have the right to obtain from the controller the blocking of data where:
(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the data,
(b) the controller no longer needs them for the accomplishment of its tasks but they have to be maintained for purposes of proof,
(c) the processing is unlawful and the data subject opposes their erasure and demands their blocking instead...".

Under Article 15 of the Regulation, data subjects have the right to have their personal data **blocked** under certain circumstances. The right of blocking (like the right to erasure) may be complementary to the right of rectification.

The EDPS considered that in certain situations, the right of rectification of the data (Article 14) is exercised jointly with the right of blocking of these data (Article 15), for example when the data subject disputes their accuracy[52]. During the period in which the controller is allowed to check the accuracy of the data, these must be blocked (at the request of the data subject).

"The data subject shall have the right to obtain from the controller the blocking of data where: ... (b) the controller no longer needs them for the accomplishment of its tasks but they have to be maintained for purposes of proof,...".

This alternative applies where data need to be deleted because the time-limit for storing them has come to end, but the data subject needs the data to prove a right in Court or in another proceeding (Article 90 of the Statute, complaint with the European Ombudsman, etc.).

The EDPS has highlighted that two situations need to be distinguished[53]:

1) Where data subjects contest the **accuracy** of the data relating to them, the data must be blocked 'for a period enabling the controller to verify the accuracy, including the completeness, of the data'. Consequently, where the controller receives a request for blocking on those grounds, the data must be immediately blocked for the period necessary to verify the accuracy and completeness of the data[54].

2) Where data subjects request the blocking of their data on grounds of **unlawful processing** or where the data must be blocked for **purposes of proof**, the controller will need a certain amount of time to conduct this assessment in order to decide whether the data should be blocked. In this case, even though the data cannot be blocked immediately, the request must be processed promptly in order to protect the data subject's rights. The EPDS therefore considers that such requests

[52] See cases 2007-0218 and 2007-0063.
[53] See case 2010-0796.
[54] See also case 2011-0483.

should be assessed as quickly as possible and, at the latest, within 15 working days.

"2. In automated filing systems blocking shall in principle be ensured by technical means. The fact that the personal data are blocked shall be indicated in the system in such a way that it becomes clear that the personal data may not be used".

In line with the concept of "privacy by design", new systems should include blocking or flagging capabilities. The EDPS recommends that systems include the possibility to block individual data without blocking the whole system[55]. Where complete blocking would paralyse the entire processing system, the EDPS recommends continuing the processing, but taking a snapshot of the data by means of a printout, a backup or a CD ROM in order to document the status quo at the time of the request. Three copies should be made, one for the data subject requesting the blocking, one for the controller and one for the DPO of the institution (or DPC, where applicable), so as to facilitate the latter's intervention in the case of a complaint[56].

4. Erasure, Article 16 of the Regulation

"The data subject shall have the right to obtain from the controller the erasure of data if their processing is unlawful, particularly where the provisions of Sections 1, 2 and 3 of Chapter II have been infringed".

Under Article 16 of the Regulation, data subjects have the right to obtain the erasure of their personal data if their use is unlawful.

The processing operation may be **unlawful** because there is no legal basis under Article 5 of the Regulation or because there has been a breach of the Regulation by the controller.

The EDPS has clarified that where according to a particular retention policy certain personal data need to be retained, it is possible to erase these before the end of the established retention period where they have been *unlawfully* processed[57]. This is because, under such circumstances, erasure represents a measure adopted in order to ensure compliance with the Regulation[58].

[55] See the case of Sysper 2, 2006-0436, in the context of a rectification request.
[56] See cases 2006-0436 and 2007-0218.
[57] See case 2009-0550.
[58] The CJEU has established (case F-130/07) that the grounds for considering a processing "*unlawful*" are not limited to a breach of Sections 1, 2 and 3 of Chapter II of the Regulation ("...*il ne peut être interprété, eu égard aux termes dans lesquels il est formulé et notamment à l'emploi de l'expression « en particulier », comme limitant le contrôle de la légalité de ces traitements au seul respect des dispositions des sections du règlement n° 45/2001 qu'il mentionne. Pour autant, tout moyen tiré de l'illégalité d'un des traitements en cause ne saurait être regardé comme opérant...*").

The right of erasure is (like the right to blocking) complementary to the right of rectification and frequently granted at the same time.

The EDPS usually recommends that EU institutions decide on whether to erase the data as soon as possible, but at the latest within 15 working days.

Administrative inquiries and disciplinary procedures

As noted in the EDPS Guidelines on administrative inquiries and disciplinary proceedings (p.5), according to Article 27 of Annex IX to the Staff Regulations, certain information may at the discretion of the Appointing Authority be removed from the personal file[59]. The data subject is therefore not granted with an automatic removal of the data after a certain lapse of time. This must be reconciled with the principles set out in the Regulation. In consequence, for data processing to be 'fair', the Appointing Authority must justify the reasons for which the data are being kept and any refusal to erase data where the data subject so requests.

Blacklisting/asset freezing

In the case of asset freezing, if a review procedure leads to the conclusion that a person's data has been stored unlawfully pursuant to Article 16 of the Regulation, additional measures on top of a simple removal from the list would have to be taken, in order to publicly "clear" the names of wrongfully listed persons[60]. As it is not possible to remove data from the official record in the Official Journal once published, a *corrigendum* stating that a person had been unlawfully included in the list should be published in the Official Journal. This is to be distinguished from cases in which the initial decision to list was lawful, but the person is removed at a later stage when new information has become available (e.g. after charges have been dropped against persons listed under Regulation 2580/2001).

5. Notification to third parties, Article 17 of the Regulation

"The data subject shall have the right to obtain from the controller the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking pursuant to Articles 13 to 16 unless this proves impossible or involves a disproportionate effort".

Under Article 17 of the Regulation, data subjects who have obtained the rectification, erasure or blocking of their data also have the right to demand that the controller **notifies third parties** to whom these data have been disclosed.

[59] Article 27 of Annex IX to the Staff Regulations reads: "*An official against whom a disciplinary penalty other than removal from post has been ordered may, after three years in the case of a written warning or reprimand or after six years in the case of any other penalty, submit a request for the deletion from his personal file of all reference to such measure. The Appointing Authority shall decide whether to grant this request*".

[60] See case 2010-0426.

Article 17 is typically used in the case of complaints[61]. The notification to third parties contributes to the **fair** processing of the data (**Article 4(1)(a) of the Regulation**). In certain cases, a rectification of data without notification to the third party would be useless for the data subject.

6. The right to object, Article 18 of the Regulation

> *"The data subject shall have the right:*
> *(a) to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her, except in the cases covered by Article 5(b), (c) and (d). Where there is a justified objection, the processing in question may no longer involve those data; ...".*.

The wording of Article 18 of the Regulation would suggest that the data subjects' right to object to the processing of data relating to them is excluded in cases where the data subjects have previously given their **consent under Article 5(b) of the Regulation**. This interpretation is too strict: for consent to be "freely given", withdrawal should always be made possible[62].

The right to object may only be applied on **compelling legitimate grounds**. The EDPS has found that such grounds exist in the following cases:

- where the data subject has objected to the publication of his or her names being mentioned in decisions by national courts published on the internet by an EU agency[63];
- where experts appointed as members of an Advisory Scientific Committee request that their names are not made publicly available on a website. If such a case occurs, the EDPS takes the view that the body will need to take necessary measures to weigh up the compelling and legitimate interests that the expert might evoke (e.g. scientific rivalry) against the interests of transparency of the public mandate of the body[64].

In contrast, the EDPS has found that **no compelling legitimate ground** exists when the data subject has objected to:

- the publication of the data subject's name as contact person in a tendering register of the EU;
- the disclosure to a third party that the data subject was a civil servant at an EU institution in the context of civil proceedings[65]. In this case,

[61] See e.g. case 2007-0029.
[62] See the WP 29 Opinion on the consent, 15/2011: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.
[63] As regards the CJEU *acting its judicial capacity*, Article 46(c) stipulates that the EDPS shall "*monitor and ensure the application of the provisions of this Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity*".
[64] See case 2011-0101.
[65] See case 2008-0600.

the person concerned objected to the disclosure of such information and lodged a complaint with the EDPS. The EDPS did not find any legitimate compelling ground to object to such transfer of information;

- the disclosure of salary details to the data subject's spouse in the context of divorce proceedings.

The EDPS has pointed out that, in the course of an **inspection, on-the-spot check or forensic operation**, it is not uncommon that the person concerned alleges that certain data cannot be collected because this would infringe data protection legislation[66]. Internal rules applicable to such procedures should therefore contain a reference to the right of the parties to object on compelling legitimate grounds under Article 18 of the Regulation. They should also stipulate an effective mechanism for dealing with data protection claims made during the acquisition of digital evidence on the basis of a reasonable balance between the rights of the parties involved and the efficacy of investigations. In particular, the right of the parties to have recourse to a Court and apply for interim measures in the contested cases must be preserved.

Ensuring the data subject's right to object is part of the proactive approach recommended by the EDPS in his paper on "***Public access to documents** containing personal data after the Bavarian Lager ruling*". This stated that controllers should: (i) analyse, at the time the personal data are collected, if they could be the object of a public access request. If so, they should (ii) inform the data subject about this potential disclosure and (iii) ensure his right to object. Information given to the data subject must include his/her right to object in accordance with Article 11 (f): "the controller shall provide a data subject (...) with **any further** information (...) insofar as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee **fair** processing in respect of the data subject".

"The data subject shall have the right ... (b) to be informed before personal data are disclosed for the first time to third parties or before they are used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosure or use. ...".

This provision is specific to direct marketing and only applies in such circumstances.

7. Special rights in case of automated individual decisions, Article 19 of the Regulation

"The data subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or

[66] See cases 2011-1127 to 1132.

conduct, unless the decision is expressly authorised pursuant to national or Community legislation or, if necessary, by the European Data Protection Supervisor. In either case, measures to safeguard the data subject's legitimate interests, such as arrangements allowing him or her to put his or her point of view, must be taken".

As regards the notion of a decision "based solely on **automated processing**", the equivalent provision in Art. 15 of Directive 95/46/EC[67] indicates that this refers to a decision taken without the actual input of human judgement. When the data subject can actually review the decision, Article 15 of Directive 95/46/EC no longer applies[68].

The EDPS has stressed that it is crucial that data subjects are granted the rights to access and rectify material errors in respect of all data generated on an automatic basis[69]. The EDPS has further underlined that staff members must understand the logic involved in the processing so that they can understand how such data are generated, and have them rectified if they are not correct. Moreover, guarantees should be put in place to ensure that the data subjects' legitimate interests are taken into account. In particular, in terms of the evaluation aspects, employees should be granted the right to provide justification for certain figures so that the performance calculation can be adjusted in an accurate manner, or to contest the accuracy of the data generated automatically prior to the evaluation exercise.

Part 2: Exceptions and restrictions

Section 6 of the Regulation stipulates certain exemptions and restrictions applicable to data subjects' rights under **Article 20(1) of the Regulation**.

"*The Community institutions and bodies may restrict the application of Article 4(1), Article 11, Article 12(1), Articles 13 to 17 and Article 37(1) where such restriction constitutes a necessary measure to safeguard:*
(a) the prevention, investigation, detection and prosecution of criminal offences;
(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters;
(c) the protection of the data subject or of the rights and freedoms of others;
(d) the national security, public security or defence of the Member States;
(e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b)".

However, as exceptions to the general rules, these limitations must be interpreted restrictively and applied on a case by case basis, never

[67] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[68] See also *A Business Guide to Changes in European Data Protection Legislation*, p. 75.
[69] See case 2011-0483.

automatically and wherever possible after the consultation of the DPO[70]. Data subjects' rights **must not be restricted more broadly than necessary**.

Regarding calls for expression of interest, the EDPS has pointed out that Article 20 (1) of the Regulation *"...may imply that access should be granted neither to the comparative data concerning other applicants (comparative results), nor to the individual opinions of the members of the evaluation or selection committees if such access would undermine the rights of others applicants or the freedom of members of the evaluation or selection committees. In any case the data subjects should be provided with aggregated results and informed of the principal reasons on which the application of the restriction of their right of access is based and of their right to have recourse to the EDPS as required by Article 20(3) of Regulation (EC) 45/2001"*[71].-

If one of the above restrictions applies, data subjects have to be informed of the principal reasons for this restriction and of their right to have recourse to the EDPS under **Article 20(3) of the Regulation**.

Article 20(4) of the Regulation establishes that in these cases, when investigating complaints by data subjects, the EDPS shall only inform the data subject whether data have been processed correctly and, if not, whether the necessary corrections have been made.

Under **Article 20(5) of the Regulation**, the provision of this information may be deferred if it would make the policy for applying the restriction ineffective (for instance, if giving the information would cause a risk of destruction of evidence in case of an investigation)[72].

Article 20(1)(a) of the Regulation: "...prevention, investigation, detection and prosecution of criminal offences"

"The Community institutions and bodies may restrict the application of ...Articles 13 to 17...where such restriction constitutes a necessary measure to safeguard: (a) the prevention, investigation, detection and prosecution of criminal offences; ...".

Whilst the wording of Article 20(1)(a) of the Regulation refers only to the investigation of *criminal offences*, the EDPS considers that it has to be interpreted in the light of the *ratio legis* of the provision, and in particular in the light of Article 13 of Directive (EC) 95/46, so as to provide for certain restrictions on the duty to inform the data subject as a measure preliminary to an internal inquiry (detection of an infringement)[73].

Article 20(1)(a) of the Regulation consequently also covers **disciplinary proceedings and administrative enquiries**. It therefore applies, for

[70] See e.g. case 2010-0598.
[71] See case 2011-0103.
[72] See also joint cases 2010-0797 to-0799 and case 2010-0598..

[73] See EDPS Guidelines on administrative inquiries and disciplinary proceedings, p. 9 and case 2005-0376.

example, to investigations carried out by the European Anti-fraud Office (OLAF) or the Commission's Investigation and Disciplinary Office (IDOC).

The Regulation must be read in the light of Directive (EC) 95/46. Indeed, paragraph 12 of the recitals of the Regulation advocates the "*consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data*". Article 13 of Directive (EC) 95/46 provides for exemptions and restrictions to certain rights "*when such a restriction constitutes a necessary measure to safeguard... d) the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions*". Article 13(d) of Directive (EC) 95/46 is far reaching and extends from the prevention, investigation, detection and prosecution of criminal offences to breaches of ethics for regulated professions. Therefore, although not explicitly mentioned, there is no reason to believe that breaches of professional duties by public sector agents are not also included in this restriction.

Temporary exception: It should be underlined that the actual need to withhold this information must be clearly demonstrated ("clear suspicions") and that the withholding of the information can only last for a defined period. This implies that the initial decision to withhold the information needs to be reviewed periodically[74]. The information must be provided to the data subject as soon as this can no longer endanger the detection of an infringement.

In cases involving **OLAF investigations**, the EDPS has pointed out that *"...Providing information to the data subject while the investigation is still ongoing could jeopardise the success of said investigation, which is why a deferral of access might be justified in these cases. However, any deferral must be decided on a case-by-case basis. These provisions may not be used to deny access systematically. Information has to be supplied to the data subject as soon as these exemptions no longer apply. Even if one of the exemptions under Article 20(1) applies, Article 20(3) obliges the controller to inform the data subject of the principal reasons for deferring access and the right to seek recourse to the EDPS. Article 20(4) establishes that in these cases, when investigating complaints by data subjects, the EDPS shall only inform the data subject whether data have been processed correctly and if not, whether the necessary corrections have been made. According to Article 20(5), this information may be deferred as long as it would deprive the restriction imposed under Article 20(1) of its effect*"[75].

Article 20(1)(b) of the Regulation: "...an important economic or financial interest...".

"The Community institutions and bodies may restrict the application of ...Articles 13 to 17...where such restriction constitutes a necessary measure to safeguard: ...
(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters; ...".

[74] See case 2011-1127, not public.
[75] See joint cases 2010-0797, 2010-0798 and 2010-0799.

The EDPS dealt with a case where grant and procurement award procedures, limited the right to rectify, insofar as the right could only be exercised up to the closing date for submission of applications or tenders[76]. In this case, the EDPS considered that the limitation of the rectification right could be considered as justified in light of Article 148(3) (now: Article 112) of the Financial Regulation which aims to ensure transparency and equality of treatment. It was concluded that the limitation was therefore in compliance with Article 20(1)(b) and (c) of Regulation (EC) 45/2001.

Article 20(1)(c) of the Regulation: "... protection of the data subject or of the rights and freedoms of others".

"The Community institutions and bodies may restrict the application of ...Articles 13 to 17...where such restriction constitutes a necessary measure to safeguard: ...
(c) the protection of the data subject or of the rights and freedoms of others; ...".

Selection & recruitment procedures

Data subjects should in principle be given access to their evaluation results for **all stages of the selection procedure**, unless the exception of Article 20(1)(c) of the Regulation (in line with Article 6 of the Annex III to the Staff Regulations) applies[77]. **Article 6 of Annex III to the Staff Regulations** reads: "*The proceedings of the Selection Board shall be secret*".

The exception of Article 20(1)(c) of the Regulation is frequently applied to restrict the right of access under Article 13 of the Regulation in selection procedures (pre-selection tests, interviews and written examinations), with a view to protecting the **independence of the jury** (from undue influence from the controller, the candidates, or any other party), the confidentiality of the jury's deliberations, the decision-making of the Selection Committee or its individual members or to safeguard **the rights of other candidates**. As noted in the EDPS Guidelines on staff recruitment (pp. 8/9), the restriction of the right of access must not exceed what is strictly necessary to achieve the above objectives. It must therefore be ensured that:

- the objective of any confidentiality requirement is to ensure that the Selection Committee is able to maintain its impartiality and independence and is not under undue influence from the controller, the candidates, or any other party; and

- any restriction on access rights must not exceed what is absolutely necessary to achieve these objectives.

The EDPS recommended that access should be provided, upon request, to:

- the evaluation sheets drawn up by the selection boards;

[76] See case 2011-0103.
[77] See e.g. case 2011-0101.

- the “separate assessment and decision documents signed by Chairpersons - on behalf of committees” documenting the final decision of the selection board; and
- the minutes of the selection boards[78].

The protection of the impartiality and independence of the selection board, which is the reason behind the requirement of confidentiality, would be unlikely to be prejudiced if the Selection Committee disclosed to candidates, in a transparent manner, the **criteria** according to which it evaluated candidates, as well as the actual detailed marks or comments a particular candidate received from the jury as a whole with respect to each criterion[79].

However, neither comparative data concerning other applicants, nor the individual opinions of the members of the Selection Committee should be disclosed to the data subject:

- With a view to protecting data regarding other candidates (**comparative data**), it should be noted that any evaluation in a selection procedure has a comparative element to it. Any restriction should, however, not be applied more broadly than necessary[80]. In keeping with transparency, granting access to the criteria applied helps candidates to see what elements were taken into account and see that the selection board has acted fairly[81].

- This exception may further imply that access should not be granted to the **individual opinions** of the members of a selection committee, as such access may be intended to undermine the rights of other applicants or the freedom of members of the selection committee[82]. Nevertheless, data subjects should be provided with **aggregated results**.

In cases regarding the selection of members of a scientific committee, the EDPS noted that the right to rectification regarding identification data was granted at any time, whereas the right to rectification of eligibility and selection data was limited until the closing date of the call for expression of interest[83]. The EDPS considered that this limitation was necessary to ensure objective, certain and stable conditions for the selection procedure, and essential to the fairness of the processing. He recognized it as a necessary measure under Article 20(1)(c) of the Regulation for the protection of the rights and freedoms of others, but noted the importance of informing all candidates about the reasons for this restriction at the time of the processing operation.

[78] See case 2007-0422.
[79] See e.g. cases 2011-0101 and 2010-0980; see case 2011-0511 for amalgamated feedback data on colleagues.
[80] See e.g. case 2011-0483.
[81] See e.g. case 2010-0980.
[82] See e.g. case 2011-0483.
[83] See cases 2011-0101 and 2010-0980.

As pointed out in the EDPS Anti-harassment Guidelines (p. 11), regarding the **selection of confidential counsellors** specifically, the EDPS is aware that a limitation to the data subject's right of access to the overall final assessment of the selection process is possible, in accordance with the principle of the secrecy of selection committee proceedings. This principle should nevertheless be read in the light of Article 20(1)(c) of the Regulation.

In addition, the EDPS notes (Anti-harassment Guidelines, p. 11) that limitations to the right of rectification of candidates' data, after the deadline for the sending of documents regarding a given selection, may be necessary for different reasons, including those of a practical nature. In this regard, the EDPS considers that these limitations can be seen as necessary to ensure objective, certain and stable conditions for the selection, and as essential to the fairness of processing. Thus it can be recognized as a necessary measure under Article 20(1)(c) of the Regulation for the protection of the rights and freedoms of others.

Medical files

Regarding personal notes of medical officers contained in medical files, the EDPS Guidelines on health data (p. 15) note that the notion of "*rights and freedoms of others*" refers to the fact that the rights and freedoms of an identified third party override the data subject's right of access to the information. This should be examined on a case-by-case basis in the light of the principle of proportionality, and precludes a blanket denial of access to personal notes of medical officers contained in medical files.

In one case, data subjects had the right of direct access to their medical file, to be exercised on the premises of the medical service in the presence of a person designated by the medical service[84]. They also had the right of indirect access in order to consult psychiatric/psychological reports through the intermediary of a doctor appointed by the data subject. In this case, the EDPS highlighted that any restriction on access to medical files should be examined on a case-by-case basis in accordance with the principle of proportionality, and that Article 20(1)(c) of the Regulation must not be allowed to result in a general refusal of access to the personal notes of doctors in the medical file.

As regards psychological or psychiatric data, the EDPS has stated that EU institutions should ensure that data subjects have indirect access, if -following a case-by-case assessment- it is considered based on Article 20(1)(c) of the Regulation that no direct access can be given in order to protect the data subject[85].

Procurement

In a case regarding grant and procurement award procedures, data subjects were granted rights of access and rectification upon request, but the right to rectify was limited and could only be exercised up to the closing date for submission of applications or tenders[86]. The EDPS considered that this

[84] See case 2011-0655.
[85] See case 2010-0071.
[86] See case 2011-0103.

limitation of the rectification right could be considered as justified in light of Article 148(3) of the Financial Regulation aiming to ensure transparency and equality of treatment and thus was compliant with Article 20(1) (b) and (c) of the Regulation.

Administrative inquiries and disciplinary procedures

As mentioned in the Guidelines on administrative inquiries and disciplinary procedures (p. 9), the EDPS considers that the exception has to be interpreted in the light of its *ratio legis*, in particular when considering that in the context of an investigation or disciplinary procedure, **data related to data subjects other than the person under investigation** may be present.

The EDPS has noted that special attention should be paid to such other possible data subjects, specifically to whistleblowers, informants or witnesses[87]. Any restriction to the right of access of these persons should be in line with Article 20 of the Regulation and their identity should be kept confidential in as much as this does not contravene national rules regarding judicial proceedings.

- On **whistleblowers**, the Article 29 Working Party has highlighted that *"[u]nder no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower from the scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower's confidentiality should always be guaranteed".* As pointed out in the EDPS Guidelines on administrative inquiries and disciplinary proceedings, p. 9), the same approach has to be applied to **informants**. Therefore, the EDPS recommends that the identity of whistleblowers and informants is kept confidential in the context of administrative inquiries and disciplinary proceedings, except for situations in which this would infringe national rules on judicial procedures and/or in case of malicious false statements[88]. In such cases, these personal data can only be disclosed to judicial authorities[89].

[87] See e.g. cases 2010-0752 and 2011-0806 and EDPS Guidelines, p. 9.

[88] See case 2011-1127, not public). This refers to principles and rules of civil and/or criminal law protecting against slanderous accusations, a point that should be read in combination with the national rules applicable to judicial procedures in Member States. Where these foresee the possibility of revealing the identity of whistleblowers or informants, account should be taken of Article 8(a) of the Regulation. In this case, the recipient (i.e. the judicial authorities) would have to demonstrate that the data required are "*necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority*". Furthermore, Article 8 stipulates that the requisites mentioned in paragraph (a) are to be applied without prejudice to Articles 4, 5, 6 and 10 of the Regulation. Article 5 requires the existence of a legal basis for the processing (in the case under analysis the legal basis would be the obligation to cooperate with national judicial procedures). As Article 4 includes the data quality principle, the data transferred have to be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Article 4(1)(c)). In other words, the transfer of data should not involve more information or more detailed information than necessary for the purpose declared (case 2010-0458).

[89] See case 2010-0458 with more detail.

- In contrast, **witnesses** in principle do not require the confidentiality of their identity. However, in certain cases it might be necessary to protect their identity. This analysis has to be conducted on a case-by-case basis (EDPS Guidelines on administrative inquiries and disciplinary proceedings, p. 9).

The need for protecting whistleblowers and informants in principle remains the same after the closure of an investigation. The vulnerability of the whistleblower's or informant's role, and therefore the risks to their privacy and integrity does not change depending on whether the investigation is opened or closed with no follow-up. The protection of their "*rights and freedoms*" would therefore require a continuity of protection under Article 20(1)(c) of the Regulation[90].

Harassment

The EDPS has established that alleged harassers may have their right to access restricted if necessary to safeguard "*the protection of the data subject or of the rights and freedoms of others*"[91]. Their access is then subject to them having been informed by the controller, with the agreement of the alleged victim, of the existence of an informal procedure against them. Furthermore, Article 20(1)(c) may in certain cases also be applied to protect the rights of other persons concerned, especially witnesses. This limitation should only be applied when strictly necessary to protect the rights and freedoms of others, and in order to secure the good administration of cases or the future relations of the parties.

Access to documents under Regulation (EC) No. 1049/2001

Under Article 4(1)(b) of Regulation (EC) No. 1049/2001, "*The institutions shall refuse access to a document where disclosure would undermine the protection of: [...] (b) privacy and integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data...*". The relevant rules on data protection referred to in this provision are laid down in Regulation (EC) No 45/2001, including Articles 8(b) and 20 (1)(c). For further guidance on the relationship between the two Regulations in the light of the case law of the Court of Justice, please refer to the **EDPS Background Paper** "*Public access to documents containing personal data after the Bavarian Lager ruling*" available on the EDPS website.

Article 20(1)(d) of the Regulation: "...the national security, public security or defence of the Member States".

The EDPS has so far not addressed this issue in any cases.

[90] See case 2010-0458.
[91] See case 2010-0598.

Article 20(2) of the Regulation

"2. Articles 13 to 16 shall not apply when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics, provided that there is clearly no risk of breaching the privacy of the data subject and that the controller provides adequate legal safeguards, in particular to ensure that the data are not used for taking measures or decisions regarding particular individuals.".

In a case regarding a study on fingerprint recognition of children under the age of 12, the EDPS noted that the conditions of Article 20(2) of the Regulation could be met[92].

Article 20(3)-(5) of the Regulation

"3. If a restriction provided for by paragraph 1 is imposed, the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor.".

In the case of harassment, the EDPS has noted that exceptions under Article 20 will most probably be used to defer the right of access of the alleged harasser to his/her own data[93]. This limitation is applied to protect the alleged victim. The right of access of the alleged harasser is linked to the information he has already received on the procedure. For example, an alleged harasser will not request access if he is not aware of an existing informal procedure involving him. The application of the limitations must be dealt with on a case by case basis by the controller taking into consideration the alleged victim's protection.

In cases involving **OLAF investigations**, the EDPS has pointed out that *"...Even if one of the exemptions under Article 20(1) applies, Article 20(3) obliges the controller to inform the data subject of the principal reasons for deferring access and the right to seek recourse to the EDPS. Article 20(4) establishes that in these cases, when investigating complaints by data subjects, the EDPS shall only inform the data subject whether data have been processed correctly and if not, whether the necessary corrections have been made. According to Article 20(5), this information may be deferred as long as it would deprive the restriction imposed under Article 20(1) of its effect*."[94].

"4. If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.
5. Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect.".

[92] See case 2011-0209.
[93] See case 2011-0483.
[94] See joint cases 2010-0797, 2010-0798 and 2010-0799.

In line with the EDPS Guidelines on administrative inquiries and disciplinary procedures (p. 10), should a restriction to the rights of access or rectification be imposed, the data subject should be informed of the principle reasons for the application of the restriction and the right to have recourse to the EDPS for **indirect access** according to Article 20(4) of the Regulation. Provision of this information may be deferred for as long as such information would deprive the restriction of its effect.

Part 3: What the EDPS does to protect data subjects' rights

The EDPS supervises the processing (collection, use, transfer, etc.) of personal data by the EU institutions and ensures the respect of data protection rights in this context. The EDPS may therefore:

- **prior check** processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes;
- **give advice**: data subjects may ask the EDPS advice on how to exercise their rights;
- **hear and investigate complaints**: if data subjects feel that their data protection rights have been infringed by the EU institutions, they can lodge a complaint with the EDPS. A complaint to the EDPS can **only** relate to a **processing of personal data**. The EDPS is not competent to deal with cases of general maladministration, to modify the content of the documents that the complainant wants to challenge or to grant financial compensation for damages. Further, the EDPS is only competent to deal with complaints involving the processing of personal data carried out by **one of the EU institutions**.

Article 47 of the Regulation attributes certain powers to the EDPS. These include the power to:

- **conduct enquiries and inspections**, on his own initiative or on the basis of a complaint, when it is necessary to obtain more information on the processing of personal data;
- **order** that requests to exercise certain rights in relation to personal data be complied with where such requests have been refused in breach of data subjects' rights;
- **warn or admonish** the EU institution or body which is unlawfully or unfairly processing personal data;
- **impose** a temporary or definitive **ban** on processing;
- **refer a case** to the Court of Justice of the European Union.

To exercise his competences, the EDPS is entitled to obtain access from the EU institution or body concerned to all personal data and to all information necessary for his enquiries. He can also have access to any EU institution's premises in case an on-the-spot investigation is needed.

Glossary

Personal data: any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

Data processing: any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

DPO: a data protection officer is appointed by every EU institution and body. The DPO has the duty to ensure, in an independent manner, the internal application of the provisions of the Data Protection Regulation (EC) 45/2001. You can consult the list of DPOs on the EDPS website: http://www.edps.europa.eu/EDPSWEB/edps/Supervision/DPOnetwork

EU institutions : all institutions, bodies, offices or agencies operating for the European Union (e.g. European Commission, European Parliament, Council of the European Union, European Central Bank, specialised and decentralised EU agencies).

Sensitive data: sensitive include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. The processing of such information is in principle prohibited, except in specific circumstances.

Controller: The EU institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data.

Further reading (1)

- **Articles 13 to 19 of Regulation (EC) No 45/2001** 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:

- Right of access: see judgement of the CJEU, C-553/07, Rotterdam v. Rijkeboer; EDPS letter of 1 October 2009 on consultation 2009-0550 on access right; access to data in EPSO competition: awaiting judgment on Pachtitis, T-374/07;
- Modalities of the right of access and restrictions on the exercise this right: EDPS thematic Guidelines on staff recruitment, health data, administrative enquiries and disciplinary proceedings, anti-harassment procedures, see also EDPS letter of 30 July 2010 on consultation on confidentiality of informants' identity (2010-0458);
- Indirect access to psychological or psychiatric data: EDPS prior checking Joint Opinion on medical data, case 2010-0071, and Conclusions 221/04 of *Collège des Chefs d'administration* of 19 February 2004;
- Blocking: EDPS prior checking Opinion on Sysper 2: Time management module, case 2007-0063, and Opinion on Flexitime at DG INFSO, case 2007-0218;
- Right of data subjects in respect of automated decision process: EDPS prior check opinion 2009-0771;
- Compelling legitimate grounds: see EPDS prior checking Opinion in case 2011-0101;
- EDPS Background Paper "*Public access to documents containing personal data after the Bavarian Lager ruling*".

(1) All the EDPS documents listed in this section are available on the EDPS website: www.edps.europa.eu .

ANNEX

List of published Opinions cited in these Guidelines	
Case number / Opinion title	**Summary**
2004-0236 Opinion on a notification for prior checking received from the Data Protection Officer of the European Commission on the system of "Recruitment, by competition, of permanent staff for the European institutions or for Community bodies, offices and agencies"	Art. 20(1)(c) in selection and recruitment procedures, aggregated results
2005-0376 Opinion on a notification for prior checking received from the Data Protection Officer of the European Central Bank on the recording, storing and listening of telephone conversations in DG-M and DG-P	Art. 20(1)(a): *ratio legis* > criminal offences
2005-0418 Opinion on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office on OLAF internal investigations	broad concept of personal data, Article 2(a) of the Regulation, qualified third party
2007-0063 Opinion on the notification for prior checking received from the Data Protection Officer of the European Commission on "SYSPER 2: Time Management Module"	blocking combined with rectification
2007-0218 Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on "the implementation of flexitime - specific to DG INFSO"	blocking combined with rectification; requirement 3 copies
2007-0422 Opinion on the notification for prior checking received from the Data Protection Officer of the European Medicines Agency ("EMEA") regarding EMEA's "Access" recruitment database and selection and recruitment procedures	Art. 20(1)(c) in selection and recruitment procedures, aggregated results
2007-0566 Opinion on the notification for prior checking received from the Data Protection Officer of the European Maritime Safety Agency on the recruitment of permanent, temporary and contract agents	Art. 14, rectification identification data
2009-0550 Consultation under Art. 46(d)[95]	right of access in OLAF investigation + level of detail; confirmation in the sense of Art. 13(1)(a)
2009-0771 Opinion on a notification for Prior Checking received from the Data Protection Officer of the Office for Harmonization in the Internal Market (OHIM) concerning "Analytical accounting and performance reports"	automated individual decision / understanding of logic involved
2010-0071 (Joint) Opinion on notifications for prior checking received from the Data Protection Officers of certain EU agencies concerning the "processing of health data in the workplace"	Art. 20(1)(c) / psychological and psychiatric data
2010-0426 European Commission Processing of personal data in connection with regulations requiring asset freezing as CFSP related restrictive	right to rectify asset freezing

[95] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2009/09-10-01_OLAF_right_access_EN.pdf.

measures	
2010-0458 Complaint case[96]	Art. 20(1)(c) whistleblowers + informants
2010-0598 Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Medicines Agency (EMA) regarding the processing operations "Listening Points/Informal procedures" (management of cases of psychological or sexual harassment).	access to data subject's data whether provided by data subject or not; exceptions under Art. 20 apply restrictively + consultation DPO, Art. 20(1)(c) harassment; Art. 20(3)-(5)
2010-0752 (Joint) Opinion on notifications for prior checking received from the Data Protection Officers of certain EU agencies concerning the "processing of administrative inquiries and disciplinary proceedings".	access and rectification disciplinary file; Art. 20(1)(c) whistleblowers
2010-0796 Temporary staff employed by the Committee of the Regions	data subject rights as enforceable rights; when to block
2010-0797 to 0799 Opinion on notifications for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office regarding the Virtual Operational Cooperation Unit, the Mutual Assistance Broker, and the Customs Information System	Art. 20(1)(a), (3)-(5)
2010-0869 Opinion on the notification for prior checking received from the Data Protection Officer of the Office for Harmonization for the Internal Market ("OHIM") concerning OHIM's Quality Management System and ex-post quality checks	controller must ensure effective use of data subject rights
2010-0914 Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Centre for Disease Prevention and Control regarding Annual Declaration of Interest	info to data subject on right to object, Art. 11(f)
2010-0980 Opinion on the notification for prior checking from the Data Protection Officer of EFSA regarding the "Selection and Appointment of members of EFSA's Scientific Committee and Panels"	access in selection procedure; disclosure of selection criteria + comparative data, Art. 20(1)(c)
2011-0101 Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Central Bank regarding the "Selection of the members of the European Systemic Risk Board Advisory Scientific Committee"	access in selection procedures; right to object; Art. 20(1)(c), disclosure of selection criteria
2011-0103 Opinion on the notification for prior checking from the Data Protection Officer of the European Environment Agency concerning "Grant and procurement award procedures including call for expression of interest"	access grant & procurement procedures; Art. 20(1)(b) + (c)
2011-0209 Opinion on a notification for prior checking received from the Data Protection Officer of the European Commission related to the "Fingerprint recognition study of children below the age of 12 years"	Art. 20(2) / study on fingerprint recognition
2011-0483 Opinion on notifications for prior checking received from the Data Protection Officers of certain EU agencies concerning the "anti-harassment policy" and "the selection of confidential counsellors"	immediate blocking if accuracy contested; disclosure of aggregated + comparative results, Art. 20(1)(c); Art. 20(3)-(5) harassment
2011-0511	rectification evaluation procedure;

[96] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2010/10-07-30_Letter_Ombudsman_EN.pdf.

Opinion on the notification for prior checking from the Data Protection Officer of the European Commission concerning Feedback for further development of DGT managers	amalgamated feedback data on colleagues, Art. 20(1)(c)
2011-0655 Opinion on the notification of a prior check received from the Data Protection Officer of the Court of Justice of the European Union ('the Court') regarding the 'Invalidity Committee Procedure'	rectification medical files; Art. 20(1)(c)
2011-0806 Opinion on the updated notification concerning administrative inquiries and disciplinary proceedings within the Court of Justice of the EU	rectification disciplinary file; Art. 20(1)(c) whistleblower, informant, witness
2011-1127 to 1132 Opinion on the notifications for prior checking from the Data Protection Officer of the European Anti-Fraud Office (OLAF) regarding new OLAF investigative procedures (internal investigations, external investigations, dismissed cases and incoming information of no investigative interest, coordination cases and implementation of OLAF recommendations)	objection mechanism inspections, forensic operations
2012-0586 Complaint case - not published	
2012-0841 Complaint case - not published	access / format, Art. 13(1)(c)