Preliminary remarks:

- *Certain Articles of the Treaty and wording of the Regulation should be updated (in particular, the term "union" should substitute the term "community").*
- *The Court of Justice of the European Union makes reference to the case law relating to the interpretation of the provisions of Directive 95/46/EC which is applicable to the interpretation of the provisions of Regulation (EC) No 45/2001 (see Commission v Germany[1])*
- *In the table below, the Articles of Regulation (EC) No 45/2001 are linked to the relevant recitals.*

ARTICLE BY ARTICLE ANALYSIS		
Chapter I GENERAL PROVISIONS		
Article 1 **Object of the Regulation**	1. In accordance with this Regulation, the institutions and bodies set up by, or on the basis of, the Treaties establishing the European Communities, hereinafter referred to as "Community institutions or bodies", shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data and shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States implementing Directive 95/46/EC. 2. The independent supervisory authority established by this Regulation, hereinafter referred to as the European Data Protection Supervisor shall monitor the application of the provisions of this Regulation to all processing operations carried out by a Community institution or body.	This Article provides for the three main objectives of Regulation (EC) No 45/2001: ▶ Protection of fundamental rights and freedoms (in particular the right to privacy) (by establishing rights for data subjects, obligations for data controllers and a supervisory body) ▶ Free flow of data ▶ Establishment of an independent supervisory authority

[1] Case C-518/07.

ARTICLE BY ARTICLE ANALYSIS		
	Recitals *(1) Article 286 [EC] requires the application to the Community institutions and bodies of the Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data.* *(5) A Regulation is necessary to provide the individual with legally enforceable rights, to specify the data processing obligations of the controllers within the Community institutions and bodies, and to create an independent supervisory authority responsible for monitoring the processing of personal data by the Community institutions and bodies.* *(9) Directive 95/46/EC requires Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, in order to ensure the free flow of personal data in the Community.* *(13) The aim is to ensure both effective compliance with the rules governing the protection of individuals' fundamental rights and freedoms and the free flow of personal data between Member States and the Community institutions and bodies or between the Community institutions and bodies for purposes connected with the exercise of their respective competences.*	
Article 2 Definitions	For the purposes of this regulation : (a) "personal data" shall mean any information relating to an identified or identifiable natural person hereinafter referred to as **"data subject"; an identifiable 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,**	▶ **The concept of personal data is interpreted broadly.** There have been several court cases relating to the interpretation of the notion of personal data (decided on the basis of Directive 95/46) such as: o *Commission v Bavarian Lager*[2]: the list of participants in a meeting organised by the Commission, which had

[2] CJEU, 29 June 2010, European Commission v. Bavarian Lager Co. Ltd., Case C-28/08 P.

ARTICLE BY ARTICLE ANALYSIS		
	cultural or social identity; **Recitals** *(7) The persons to be protected are <u>those whose personal data are processed by Community institutions or bodies</u> in any context whatsoever, for example because they are employed by those institutions or bodies.* *(8) The principles of data protection should apply to <u>any information concerning an identified or identifiable person.</u> To determine whether a person is identifiable, account should be taken of all the means likely to be reasonably used either by the controller or by any other person to identify the said person. The principles of protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.*	been attended by representatives of a business organisation, which were included in the minutes of that meeting, are personal data within the meaning of Article 2(a) of Regulation (EC) No 45/2001, since those participants could be identified (paragraph 68). ○ *Client Earth and Pesticide Action Network Europe (PAN Europe) v EFSA*[3]*-ongoing appeal*: EFSA disclosed to applicants all of the names, biographies and declarations of interest of experts on EFSA's website, as well as the comments made by the experts. Applicants want also access to **the link between each comment and its author.** This information is a "set of personal data within the meaning of Article 2(a) of Regulation (EC) No 45/2001, even if that information is held by EFSA in an employment context"(Paragraphs 46, 50-52). ○ *YS v Minister voor Immigratie, Integratie en Asiel; Minister voor Immigratie, Integratie en Asiel v M, S*[4]: "*the concept of personal data*" must be interpreted as meaning that the "*data relating to an applicant for a residence permit contained in an administrative document, such as the 'minute' at issue in the main proceedings, setting out the grounds that the case officer puts forward in support of the draft decision which he is responsible for drawing up in the context of the procedure prior to the adoption of a decision concerning the application for such a permit and,*

[3] CJEU, 13 September 2013, ClientEarth and PAN v EFSA, Case T-214/11. An appeal is currently pending before the Court of Justice (Case C-615/13 P).
[4] CJEU, 17 July 2014, YS v Minister voor Immigratie, Integratie en Asiel; Minister voor Immigratie, Integratie en Asiel v M, S, Cases C-141/12 and C-372/12.

ARTICLE BY ARTICLE ANALYSIS		
		where relevant, the data in the legal analysis contained in that document, are 'personal data' within the meaning of that provision, whereas, by contrast, that analysis cannot in itself be so classified (paragraph 48)"
	(b) "processing of personal data" hereinafter referred to as "processing" shall mean any operation or set of operations which is 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;	▶ **The Court of Justice has provided guidance on the concept of processing of personal data, such as:** ○ *Bodil Lindqvist*[5]: *"the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes* ***the processing of personal data wholly or partly by automatic means*** *(paragraph 27)."* ○ *Commission v Nanopoulos*[6]: *"an unlawful leaking of personal information is a processing of personal data contrary to the provisions of Regulation (EC) No 45/2001 (paragraph 160 - F-30/08)."*
	(c) "personal data filing system" hereinafter referred to as "filing system" shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;	▶ No particular comment is called for.
	(d) "controller" shall mean the Community institution or body, the	▶ The definition of the controller has raised interpretation

[5] CJEC, 6 November 2003, Bodil Lindqvist, Case C-101/01.

6 CJEU, 11 May 2010, Fotios Nanopoulos v European Commission, Case F-30/08and confirmed on appeal T-308/10 P. See also CJEC, 12 September 2007, Kalliopi Nikolaou v Commission, C-259/03.

ARTICLE BY ARTICLE ANALYSIS		
	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;	issues as it is unclear whether the controller is the institution/body, the unit/division, or the DG. The EDPS and the EU bodies consider that the controller is always the institution or body and not the natural person who determines the means and purposes of the processing and who is designated as the data controller (*e.g.* in the notification). ▶ The definition of the controller is unclear and inconsistent throughout the Regulation. In Article 2. (d), it appears that the controller is the institution /body or the units/services/directorates within the EU institution or body. However, pursuant to Article 25, the name and address of the controller appearing in the registers are the details of the natural person responsible for the processing operation. ▶ This question is directly linked to responsibility for the processing operation. Under the current system, the EU body bears the responsibility while data controllers may only be subject to disciplinary proceedings in cases of negligence or intentional harm (*see* Article 49 of the Regulation).
	(e) "processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	▶ The Data Protection Officers (DPOs) network has underlined that it is unclear whether, when this definition is construed in accordance with ArticlesArticle 21 and 23, the processor is the EU official acting on instruction of his hierarchy or an EU body/external entity acting on behalf of controllers under a contract. In the evaluator's opinion, the processor should be the EU body/external firm acting on instruction of the controller and not the team working for a data controller. The current practice is to consider that the processor is the external service provider or another EU institution/body acting on behalf and under the instruction of an EU institution or body (except for certain institutions such as the European Commission where one unit may be processing personal data

ARTICLE BY ARTICLE ANALYSIS		
		for another). An official acting under the authority of his or her hierarchy is never considered to be a processor. ▶ This definition applies to both internal service providers (e.g. an EU institution acting as a service provider for another EU body) and to external service providers selected on the basis of procurement procedures.
	(f) "third party" shall mean a natural or legal person, public authority, agency or body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;	▶ No particular comment is called for.
	(g) "recipient" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;	▶ There is an issue of interpretation of the definition of recipient concerning which bodies should be considered as an *"authority which may receive the data in the course of an inquiry"*, notably in light of the application of Articles 7, 8 and 9 on transfer of personal data. Some EU institutions and bodies have interpreted this exception as also covering the rules on transfer. The EDPS took the view that only Articles 11 and 12 on information on data subjects do not apply to authorities which receive data within the framework of a particular inquiry. The rules on transfers apply to these authorities. ▶ Moreover, it is unclear whether the *"authorities which may receive data in the framework of a particular inquiry"* refer to EU bodies or to authorities that are subject to Directive 95/46/EC or even authorities in third countries. ▶ The definition does not exclude the processor as a recipient; it is unclear whether the processor should be considered as a recipient. Moreover, it could be argued that this non-inclusion of the processor among the recipients hinders the application of the rules on transfer of personal data (Articles 7, 8, 9). For

ARTICLE BY ARTICLE ANALYSIS		
		the EDPS, the processors are recipients and rules relating to transfers apply when the data is transferred to a processor.
	(h) "the data subject's consent" shall mean any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed.	**Application** ▶ Consent is rarely used by EU institutions and bodies as a legal basis for a data processing operation (for example, the use of the photographs of EU officials).
Article 3 **Scope**	1. This Regulation shall apply to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law. 2. This Regulation shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. **Recitals** *(14) To this end measures should be adopted which are binding on the Community institutions and bodies. These measures should apply to all processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.* *(15) Where such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this*	▶ *Commission v Bavarian Lager*[7]*: "Where a request based on Regulation No 1049/2001 seeks to obtain access to documents including personal data, the provisions of Regulation (EC) No 45/2001 become applicable in their entirety, including Articles 8 and 18 thereof"* (paragraph 63). *See Recital 15.* ▶ *Cf.* case study on Data Protection in the ex-third pillar with regard to the application of the Regulation to the bodies in the area of Police and Judicial Cooperation in criminal matters

[7] CJEU, 29 June 2010, European Commission v. Bavarian Lager Co. Ltd., Case C-28/08 P.

ARTICLE BY ARTICLE ANALYSIS		
	Regulation, in particular those laid down in Titles V and VI of the Treaty on European Union, the protection of individuals' fundamental rights and freedoms shall be ensured with due regard to Article 6 of the Treaty on European Union. Access to documents, including conditions for access to documents containing personal data, is governed by the rules adopted on the basis of Article 255 of the EC Treaty the scope of which includes Titles V and VI of the Treaty on European Union. *(16) The measures should not apply to bodies established outside the Community framework, nor should the European Data Protection Supervisor be competent to monitor the processing of personal data by such bodies.* *(17) The effectiveness of the protection of individuals with regard to the processing of personal data in the Union presupposes the* ***consistency of the relevant rules and procedures applicable to activities pertaining to different legal contexts.*** *The development of fundamental principles on the protection of personal data in the fields of judicial cooperation in criminal affairs and police and customs cooperation, and the setting-up of a secretariat for the joint supervisory authorities established by the Europol Convention, the Convention on the Use of Information Technology for Customs Purposes and the Schengen Convention represent a first step in this regard.* *(18) This Regulation should not affect the rights and obligations of Member States under Directives 95/46/EC and 97/66/EC. It is not intended to change existing procedures and practices lawfully implemented by the Member States in the field of national security, prevention of disorder or prevention, detection, investigation and prosecution of criminal offences in compliance with the Protocol on Privileges and Immunities of the European Communities and with international law.* *(36) This Regulation does not aim to limit Member States' room for*	

ARTICLE BY ARTICLE ANALYSIS		
	manoeuvre in drawing up their national law on data protection under Article 32 of Directive 95/46/EC, in accordance with Article 249 of the Treaty.	
Chapter II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA		
Section 1 PRINCIPLES RELATING TO DATA QUALITY		

Article 4
 	
Data quality
	1. Personal data must be:
	
	(a) processed fairly and lawfully;
	
	(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. **Further processing of personal data for historical, statistical or scientific purposes shall not be considered incompatible provided that the controller provides appropriate safeguards, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual;**
	
	(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
	
	(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
	
	(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. **The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the**
		▶ This provision sets out the main data protection obligations for data controllers.
		
		Implementation and application
		
		▶ Processes/procedures have been established in more than 69% of the EU institutions and bodies.
		▶ Stakeholders underlined that the procedures and guidelines relating to data protection principles are not always suitable for meeting operational needs and are considered to be theoretical (rather than practical).
		▶ In practice, the principles are broadly applied but there are some hurdles to be overcome:
		  ○ The principles enshrined in Article 4 are well understood by DPOs overall, but the principle of "fair" processing needs to be clarified.
		  ○ There is a lack of guidance on data protection retention periods and what should be considered as a reasonable period.
		▶ The analysis of legal feasibility is often performed during the notification of the processing operations, but notification appears to be burdensome and bureaucratic and does not necessarily result in the correct application of data protection principles.
		▶ Data controllers are often not sufficiently aware of data protection requirements and obligations. They rely

ARTICLE BY ARTICLE ANALYSIS		
	data shall not be used for any purpose other than for historical, statistical or scientific purposes. 2. It shall be for the controller to ensure that paragraph 1 is complied with.	extensively on the DPOs while they bear the responsibility of verifying compliance with data protection principles. ▶ The application of the rules on the processing of personal data for historical, statistical or scientific use has led to difficulties with respect to (i) the Archive Regulation (see evaluation question on coherence); (ii) to the need to anonymize or encrypt the personal data included in the document kept for historical purposes. ▶ It has been pointed out by some stakeholders that Article 4.1(e) should be modified in order to allow storage of data for historical use without the data being anonymized, with the aim to preserve the historical value of the information. This would bring the Regulation into alignment with the current practice for the historical archives. **Recommendations** ▶ There is a need to adopt simplified procedures targeting data controllers' concrete needs rather than publishing theoretical procedures relating to data protection procedures (e.g. compliance check lists to enable data controllers to assess the legal feasibility of the processing operation and guidance relating to data retention periods). ▶ The principle of "fair" processing in Article 4 needs to be clarified.
Section 2 CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE		
Article 5 **Lawfulness of processing**	Personal data may be processed only if: (a) processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or	**Implementation** ▶ *See Article 4*: the applicable processes/procedures are the same.

ARTICLE BY ARTICLE ANALYSIS		
	in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed, or (b) processing is necessary for compliance with a legal obligation to which the controller is subject, or (c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or (d) the data subject has unambiguously given his or her consent, or (e) processing is necessary in order to protect the vital interests of the data subject.	**Application** ▶ EU institutions and bodies may face difficulties in interpreting the provisions of Article 5, notably with regard to the assessment of the legal basis of the processing operations (Article 5 (b)). ▶ The most commonly-used basis is 5 (a) and 5 (b). Articles 5 (c), (d), (e) are of limited use. Sometimes two criteria are used (e.g. consent and performance of tasks in the public interest). Only 31% of the data controllers surveyed consider that EDPS guidance is useful and well understood. ▶ Analysis of legal feasibility is often performed during the notification of the processing operations, but notification appears to be burdensome and bureaucratic and does not necessarily result in the correct application of data protection principles. ▶ Data controllers are often not sufficiently aware of data protection requirements and obligations. They rely extensively on the DPOs while they bear the responsibility of verifying compliance with data protection principles.
Article 6 **Change of purpose**	Without prejudice to Articles 4, 5 and 10: 1. Personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the **internal rules** of the Community institution or body. 2. Personal data collected exclusively for ensuring the security or the control of the processing systems or operations shall not be used for any other purpose, with the exception of the prevention, investigation,	▶ Article 6 does not define the meaning of internal rules. **Case law** – *V. v European Parliament*[8]: a mere practice is not an internal rule. It appears that these rules should be in a written form (paragraph 119). **Implementation and application**

[8] CJEU, European Union Civil Service Tribunal, 5 July 2011, V. v. European Parliament, Case F-46/09 .

ARTICLE BY ARTICLE ANALYSIS		
	detection and prosecution of serious criminal offences.	▶ The change of purpose provision is rarely implemented and applied throughout EU institutions and bodies (cf. notably paragraph 2). ▶ The provision has raised interpretation problems as there is no definition of internal rules, which creates legal uncertainty. ▶ The EDPS underlines the necessity of interpreting the change of purpose provision strictly and respecting the proportionality and necessity principles when applying it. Thus, the EDPS' interpretation is that the change of purpose provision applies solely to secondary purposes and that the adoption of internal rules is an additional safeguard in order to ensure compliance with the purpose limitation. ▶ The relevance of the provision is open to question in light of Article 4 of the Regulation (derogation from the principle of purpose limitation). **Recommendation** ▶ This provision should be clarified or deleted from Regulation (EC) No 45/2001 because (i) its deviation from the principle of purpose limitation is not supported by any legitimate grounds and (ii) the provision generates legal uncertainty.
Transfer of Personal Data **(9) Directive 95/46/EC requires Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, in order to ensure the free flow of personal data in the Community.**		
Article 7 **Transfer of personal data**	Without prejudice to Articles 4, 5, 6 and 10: 1. Personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate	**Case law** ▶ *With regard to the assessment of necessity, see V. v Parliament*[9], a case concerning the unlawful transfer of

[9] CJEU, European Union Civil Service Tribunal, 5 July 2011, V. v. European Parliament, Case F-46/09.

ARTICLE BY ARTICLE ANALYSIS		
within or between Community institutions or bodies	performance of tasks covered by the competence of the recipient. 2. Where the data are transferred following a request from the recipient, both the controller and the recipient shall bear the responsibility for the legitimacy of this transfer. The controller shall be required to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data. If doubts arise as to this necessity, the controller shall seek further information from the recipient. The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified. 3. The recipient shall process the personal data only for the purposes for which they were transmitted.	medical data relating to the pre-recruitment medical examination from the European Commission to the European Parliament: the Court ordered the European Parliament to pay damages. **Implementation and application** ▶ 59% of EU institutions and bodies consulted have implemented processes/procedures or internal rules on the transfer of personal data. ▶ This articleArticle is applicable to transfers to EU bodies located outside the EU. This aArticle is not applicable to transfers to EUROPOL and EUROJUST. ▶ The wording of the provision has given rise to interpretation issues. DPOs and data controllers face difficulties in determining the extent to which Article 7 is applicable within EU institutions. The threshold for establishing whether Article 7 is applicable to the disclosure of personal data within the same EU institution or body (e.g. between two officials of the same unit) is difficult to assess. This is partially due to the absence of legal definition of "transfer of personal data". See EDPS Guidelines on transfer to third countries and CJUE, *Bodil Lindqvist*[10]. The EPDS has called for a definition of this notion in the context of data protection reform. **Recommendation** ▶ The conditions governing the transmission of personal data within EU institutions and bodies should be clarified.

[10] CJEC, 6 November 2003, Bodil Lindqvist, Case C-101/01.

ARTICLE BY ARTICLE ANALYSIS		
Article 8 **Transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC**	Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC, (a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or (b) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.	**Case law** ▶ Concerning the assessment of the criterion of necessity, the Court of Justice of the European Union seeks to confirm whether the recipient has an *"express and legitimate justification or any convincing argument in order to demonstrate the necessity for those personal data to be transferred"* and *"whether there is any reason to assume that the data subjects' legitimate interests might be prejudiced"* (*Commission v Bavarian Lager, paragraph 78)*[11]. The Court of Justice has adopted a restrictive interpretation of the criteria of necessity. *Cf.* Access to document case study ▶ This provision has raised significant articulation issues with the provisions laid down by Regulation (EC) No 1049/2001. Several cases have been heard before the General Court on the relationship between public access to documents and data protection in particular: *British American Tobacco v. Commission*[12], *Valero Jordana v Commission*[13], *Bavarian Lager v Commission*[14], *Suárez v Council*[15], *Dennekamp v Parliament*[16], *Egan and Hackett v Parliament*[17], *Dennekamp v European Parliament*[18], *Client Earth and Pan Europe v EFSA*[19];

[11] CJEU, 29 June 2010, European Commission v. Bavarian Lager Co. Ltd., Case C-28/08 P.

[12] CJEU, Order of the President of the Court, 6 September 2010, British American Tobacco (Investments) Ltd v. European Commission, Case T-170/03.

[13] CJEU, 7 July 2011, Gregorio Valero Jordana v European Commission, Case T-161/04.

[14] CJEC, 8 November 2007, The Bavarian Lager v Commission of the European Communities, Case T-194/04, and the subsequent appeal before the Court of Justice, CJEU, 29 June 2010, European Commission v Bavarian Lager Co. Ltd., Case C-28/08 P.

[15] CJEU, Order of the President of the 8th Chamber of the Court, 10 January 2011, Angel Coedo Suarez v. Council of the European Union, Case T-3/08.

[16] CJEU, 23 November 2011, Dennekamp v Parliament T-82/09.

[17] CJEU, 28 March 2012, Kathleen Egan and Margaret Hackett v European Parliament, Case T-190/10.

ARTICLE BY ARTICLE ANALYSIS		
		Implementation and application ▶ The wording of Article 8 provides only for a situation in which the recipients request the transfer of personal data and does not provide for the rules applicable when an EU institution or body initiates the transfer. The EDPS needed to fill in this gap. ▶ 59% of EU institutions and bodies consulted have implemented processes/procedures or internal rules on the transfer of personal data. ▶ The burden of proof of the necessity of the transfer rests on the recipient. ▶ The question has been raised whether Article 8 or Article 9 applies to the transfer of personal data to national authorities from the ex-third pillar. The EDPS considered that the EU institution or body concerned must verify whether the Member State has implemented Directive 95/46/EC with regard to these authorities. Should this be the case, Article 8 is applicable. If the opposite is true, Article 9 is applicable. The adequacy should nonetheless be presumed as all Member States have signed Convention 108.[20]
Article 9 **Transfer of personal data to recipients, other**	1. Personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to	**Case law** ▶ *Cf*. CJUE, *Bodil Lindqvist*[21]: *"There is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where* ***an individual in a Member State loads personal***

[18] CJEU, 8 April 2014, European Commission v Hungary, Case C-288/12 CJEU, Dennekamp v European Parliament, Case T-115/13, pending (pleading of the EDPS before the General Court, Luxembourg, 19 November 2014).

[19] CJEU, 13 September 2013, ClientEarth and PAN v EFSA, Case T-214/11. An appeal is currently pending before the Court of Justice (Case C-615/13 P).

[20] Letter from Sophie Louveaux and Hielke Hijmans to Marie-Hélène Boulanger dated 2 October 2013.

[21] CJEC, 6 November 2003, Bodil Lindqvist, Case C-101/01.

ARTICLE BY ARTICLE ANALYSIS		
than Community institutions and bodies, which are not subject to Directive 95/46/EC	allow tasks covered by the competence of the controller to be carried out. 2. The adequacy of the level of protection afforded by the third country or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organisation, the rules of law, both general and sectoral, in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third country or international organisation. 3. The Community institutions and bodies shall inform the Commission and the European Data Protection Supervisor of cases where they consider the third country or international organisation in question does not ensure an adequate level of protection within the meaning of paragraph 2. 4. The Commission shall inform the Member States of any cases as referred to in paragraph 3. 5. The Community institutions and bodies shall take the necessary measures to comply with decisions taken by the Commission when it establishes, pursuant to Article 25(4) and (6) of Directive 95/46/EC, that a third country or an international organisation ensures or does not ensure an adequate level of protection. 6. By way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if: (a) the data subject has given his or her consent unambiguously to the proposed transfer; or	***data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.***" **Implementation and application** ► 59% of EU institutions and bodies consulted have implemented processes/procedures or internal rules on the transfer of personal data. ► This provision has raised difficulties of interpretation. The EDPS has therefore published guidelines (see EDPS Guidelines on transfer to third countries). ► The article requires ArticleEU institutions and bodies to assess the level of protection provided for by recipients but they do not have the adequate resources and/or competence to do so. ► The DPOs emphasised that it would be useful to allow the possibility of using standard clauses for transfers to third countries and international organizations instead of asking the EU institutions and bodies to assess the level of adequacy. ► The EDPS has narrowed down the cases where an authorization is necessary.

ARTICLE BY ARTICLE ANALYSIS		
	(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract entered into in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which, according to Community law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in Community law for consultation are fulfilled in the particular case. 7. Without prejudice to paragraph 6, the European Data Protection Supervisor may authorise a transfer or a set of transfers of personal data to a third country or international organisation which does not ensure an adequate level of protection within the meaning of paragraphs 1 and 2, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses. 8. The Community institutions and bodies shall inform the European Data Protection Supervisor of categories of cases where they have applied paragraphs 6 and 7.	**Recommendations** ▶ Simplification of the application rules should be considered. ▶ The solution provided for in Article 9.7 (notably the use of standard contractual clauses (validated by the EDPS)) could be suggested as an alternative to the self-assessment by EU institutions and bodies of the level of adequacy of the recipient. This could be an appropriate means to ease international transfers while maintaining a high level of protection of personal data.

ARTICLE BY ARTICLE ANALYSIS		
Section 3 SPECIAL CATEGORIES OF PROCESSING		
Article 10 **The processing of special categories of data**	1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited. 2. Paragraph 1 shall not apply where: (a) the data subject has given his or her express consent to the processing of those data, except where the internal rules of the Community institution or body provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his or her consent, or (b) processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof, or, if necessary, insofar as it is agreed upon by the European Data Protection Supervisor, subject to adequate safeguards, or (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent, or (d) processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims, or (e) processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Community institution or body, not subject to national data protection law by virtue of Article 4 of Directive 95/46/EC, and with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of this body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the	**Case law** ▶ See *Bodil Lindqvist*, the notion of data concerning health must be given a broad interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual (Paragraph 50). [22] ▶ The Court of Justice ruled that the derogation provided for by Article 10.3 relating to processing of personal data for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services by medical professionals cannot serve as the legal basis of a transfer of health data between EU institutions in the context of recruitment.[23] **Implementation and application** ▶ The Regulation establishes appropriate obligations for data controllers and safeguards for the processing of sensitive data. ▶ 50% of EU institutions and bodies have implemented processes/procedures/internal rules relating to the processing of sensitive data. ▶ Article 10.2 (e) raises interpretation issues relating to the meaning of *"a non-profit-seeking body which constitutes an entity integrated in a Community institution or body, not subject to national data protection law by virtue of Article 4 of Directive 95/46/EC, and with a political, philosophical, religious or trade-union aim"* and whether this provision

[22] CJEC, 6 November 2003, Bodil Lindqvist, Case C-101/01.
[23] CJEU, European Union Civil Service Tribunal, 5 July 2011, V. v European Parliament, Case F-46/09.

ARTICLE BY ARTICLE ANALYSIS		
	consent of the data subjects. 3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. 4. Subject to the provision of appropriate safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by decision of the European Data Protection Supervisor. 5. Processing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor, subject to appropriate specific safeguards. 6. The European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body. **Recitals :** *(26) Certain processing operations likely to present specific risks with respect to the rights and freedoms of data subjects are subject to prior checking by the independent supervisory authority. The opinion given in the context of such prior checking, including the opinion resulting from failure to reply within the set period, should be without prejudice to the subsequent exercise by the independent supervisory authority of its*	applies to trade unions within the EU institutional framework. ▶ Article 10.6 states that the EDPS *"shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body."* It appears that the EDPS has not issued guidelines on these conditions and generally approves the use of these personal data in its prior checking opinions. In this regard, the EDPS considers that the use of an identification number in a selection/recruitment procedure is reasonable *"insofar as it facilitates the identification of the applicant during the recruitment procedure."* ▶ **Stakeholders consulted have not raised any major difficulties pertaining to the application of the rules enshrined in Article 10.** **Recommendations** ▶ The fact that stakeholders have not raised concerns about the application of Article 10 could be an indicator that this provision is not fully or really understood/known by certain DPOs and data controllers. It is necessary to ensure that DPOs and data controllers are aware of the conditions pertaining to the processing of special data. ▶ This provision needs to be implemented according to dedicated rules; it cannot be comprehensively covered by prior checking rules. Making use of concrete, simplified procedures pertaining to these principles would significantly increase the effectiveness of the processing obligations.

ARTICLE BY ARTICLE ANALYSIS		
	powers with regard to the processing operation in question. *(27) Processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.* *(28) In certain cases the processing of data should be authorised by Community provisions or by acts transposing Community provisions. Nevertheless, in the transitional period during which such provisions do not exist, pending their adoption, the European Data Protection Supervisor may authorise processing of such data provided that adequate safeguards are adopted. In so doing, he should take account in particular of the provisions adopted by the Member States to deal with similar cases.* *(29) These cases concern the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life which are necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law or for reasons of substantial public interest. They also concern the processing of data relating to offences, criminal convictions or security measures and authorisation to apply a decision to the data subject 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.*	
Section 4 INFORMATION TO BE GIVEN TO THE DATA SUBJECT		
Article 11 **Information to be supplied where the data have been**	1. The controller shall provide a data subject from whom data relating to himself/herself are collected with at least the following information, except where he or she already has it: (a) the identity of the controller; (b) the purposes of the processing operation for which the data are intended; (c) the recipients or categories of recipients of the data; (d)	**Implementation and application** ► 66% of the EU institutions/bodies consulted have adopted procedures/mechanisms/procedures/internal rules on the information of data subjects.

ARTICLE BY ARTICLE ANALYSIS		
obtained from the data subject	whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; (e) the existence of the right of access to, and the right to rectify, the data concerning him or her; (f) any further information such as: (i) the legal basis of the processing operation for which the data are intended, (ii) the time-limits for storing the data, (iii) the right to have recourse at any time to the European Data Protection Supervisor, 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. 2. By way of derogation from paragraph 1, the provision of information or part of it, except for the information referred to in paragraph 1(a), (b) and (d), may be deferred as long as this is necessary for statistical purposes. The information must be provided as soon as the reason for which the information is withheld ceases to exist.	► Moreover, privacy statements are drawn up in order to inform data subjects (in particular on their rights and obligations). In this regard, information notices are usually drafted in the event of a new data processing operation. It should be pointed out that these notices are rarely updated as only 16% of data controllers surveyed systematically update their privacy notices. ► The perception of stakeholders is that the time spent on the drafting of privacy statements is excessive and that the new Regulation should instead focus on "real" compliance. **Recommendation** ► On this point, user-friendly information notices could enhance the effectiveness of information. This is also in line with the principle of transparent information and communication enshrined in Article 11 of the GDPR.
Article 12 Information to be supplied where the data have not been obtained from the data subject	1. Where the data have not been obtained from the data subject, the controller shall at the time of undertaking the recording of personal data or, if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, provide the data subject with at least the following information, except where he or she already has it: (a) the identity of the controller; (b) the purposes of the processing operation; (c) the categories of data concerned; (d) the recipients or categories of recipients; (e) the existence of the right of access to, and the right to rectify, the data concerning him or her; (f) any further information such as: (i) the legal basis of the processing operation for which the data are intended, (ii) the time-limits for storing the data, (iii) the right to have recourse at any time to the European Data Protection Supervisor, (iv) the origin of the data, except where the controller cannot disclose this information for reasons of professional secrecy, insofar as such further information is necessary, having regard to the specific circumstances in	► *See Article 11*

ARTICLE BY ARTICLE ANALYSIS		
	which the data are processed, to guarantee fair processing in respect of the data subject. 2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Community law. In these cases the Community institution or body shall provide for appropriate safeguards after consulting the European Data Protection Supervisor.	
Section 5 RIGHTS OF THE DATA SUBJECT **Recital** (22) The rights accorded the data subject and the exercise thereof should not affect the obligations placed on the controller.		

ARTICLE BY ARTICLE ANALYSIS		
SECTION 5 RIGHTS OF THE DATA SUBJECT	**Article 13** **Right of access** 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: (a) confirmation as to whether or not data related to him or her are being processed; (b) 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; (c) communication in an intelligible form of the data undergoing processing and of any available information as to their source; (d) knowledge of the logic involved in any automated decision process concerning him or her. **Article 14 Rectification** The data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data. **Article 15 Blocking** 1. 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, or; (b) the controller no longer	**Case law** ▶ *YS v Minister voor Immigratie, Integratie en Asiel ;Minister voor Immigratie, Integratie en Asiel v M, S*[24]*: "the right of access must be interpreted as meaning that an applicant for a residence permit has a right of access to all personal data concerning him which are processed by the national administrative authorities […]. For that right to be complied with,* ***it is sufficient that the applicant be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that applicant to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him by that directive.*****"** ▶ *The Court of Justice has ruled with regard to Article 12(a) of Directive 95/46/EC (which contains a similar provision on the right of access) that it requires "Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the*

[24] CJEU, 17 July 2014, YS v Minister voor Immigratie, Integratie en Asiel; Minister voor Immigratie, Integratie en Asiel v M, S, Cases C-141/12 and C-372/12.

ARTICLE BY ARTICLE ANALYSIS		
	needs them for the accomplishment of its tasks but they have to be maintained for purposes of proof, or; (c) the processing is unlawful and the data subject opposes their erasure and demands their blocking instead. 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. 3. Personal data blocked pursuant to this Article shall, with the exception of their storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of a third party. 4. The data subject who requested and obtained the blocking of his or her data shall be informed by the controller before the data are unblocked. **Article 16 Erasure** 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. **Article17 Notification to third parties** 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. **Article 18 The data subject's right to object**	*obligation to store that information represents for the controller."*[25] **Implementation and application** ▶ EU institutions and bodies have developed specific procedures and means to implement data subjects' rights; a large majority of EU institutions[26] have drafted forms which are made available on their intranets or websites in order to allow data subjects to exercise their rights. The mechanisms in place are rarely built into the system (i.e. data subjects may rarely automatically access and rectify the data processed themselves). ▶ The scope of the right of access is wide and includes a right similar to the right to data portability in Article 13 (c). ▶ There are some drawbacks: o the number of requests is low, which could be due to a high level of protection or to poor knowledge of data protection matters. Data subjects' rights are insufficiently applied although there are specific procedures and mechanisms in place and applied in order to enable data subjects to exercise their rights and data controllers to respond to requests in a timely manner; o data subjects indicate that the replies may sometimes take too long; o information notices are rarely updated; o it is difficult to exercise rights on IT systems that existed prior to Regulation (EC) No 45/2001 (new

[25] CJEU, 23 April 2009, Falco Privatstiftung and Thomas Rabitsch v Gisela Weller-Lindhorst, Case C-533/07.
[26] 77 % of the EU institutions and bodies consulted have developed specific procedures/mechanisms/processes or internal rules relating to the rights of data subjects.

ARTICLE BY ARTICLE ANALYSIS		
	The data subject's right to object 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; (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. **Article 19 Automated individual decisions** 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 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. **Recital** (2) A fully-fledged system of protection of personal data not only requires the establishment of rights for data subjects and obligations for those who process personal data, but also appropriate sanctions for offenders and monitoring by an independent supervisory body.	systems are usually designed to take into account data protection obligations in the light of the privacy by design principle). The right not to be subject to individual automated decisions is rarely applied but is entirely relevant in the context of the development of big data. **Recommendations** ▶ The right not to be subject to individual automated decision should be supported by specific guidance. ▶ The text on the right of blocking should specify that blocking is a temporary measure or a measure undertaken when erasure is not possible. ▶ The dissemination of a data protection culture within EU institutions and bodies through the high-level management would significantly increase the enforcement of rights. The attachment of DPOs and DPCs to senior management could be a factor in promoting this goal. ▶ Old IT systems may hamper the capacity of the mechanisms in place to exercise rights as in certain circumstances the exercise of rights may require complex manual intervention. The architecture of such systems was designed before Regulation (EC) No 45/2001 existed and changes to that architecture would require significant budgetary efforts. On the other hand, new IT systems are usually designed to take data protection obligations into account in the light of the data protection by design principle.
Section 6 EXEMPTIONS AND RESTRICTIONS		
Article 20	1. The Community institutions and bodies may restrict the application of	▶ Article 20 of the Regulation provides for derogation of the

ARTICLE BY ARTICLE ANALYSIS		
Exemptions and restrictions	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). 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. 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. 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	application of Article 4 (1) (Data protection principles on data quality), Article 11 (Information to be supplied where the data have been obtained from the data subject), Article 12 (1) (Information to be supplied where the data have not been obtained from the data subject), Article 13 to 17 (Rights of data subjects), Article 37(1) (erasure or anonymisation of traffic and billing data), where such restrictions constitute a necessary measure. **Case law** ► The disclosure of testimony given during a factual inquiry into psychological harassment does not concern solely the complainant but also the members of staff alleged to have been involved and those heard in the course of the investigation. Article 20 of the Regulation is thus applicable in order to limit the complainant's right to access.[27] **Implementation and application** ► As far as we are aware on the basis of the survey and the interviews, there are no procedures specific to exceptions. ► Exceptions to Article 20 are applied by a limited number of EU institutions and bodies. ► Interpretation issues have been raised regarding the scope of the exceptions. Article 20 is applied by EU institutions but some drawbacks have been identified concerning the scope of

[27] CJEU, 12 December 2012, Cerafogli v ECB, F-43/10.

ARTICLE BY ARTICLE ANALYSIS		
	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.	the Article and its coherence with other provisions. ▶ According to the current practices of EU institutions and bodies, Article 20.1 (a) is interpreted by the EDPS as including administrative inquiries and disciplinary proceedings.[28] ▶ The exception relating to "important economic and public interest of a Member State or of the EU" seems too narrow to include all legitimate interests pursued by EU institutions or bodies, such as "**security rules with regard to the protection of EU classified information which might justify the disclosure on the basis of a request for access to personal data pursuant to Article 13.**" This reasoning could also be applied to the exceptions for "national security, public security or defence of the Member States" which could be broadened or clarified to cover the security interest of the EU institutions and bodies (notably in the event of security incidents). ▶ The DPOs have observed that in Article 20 1.c), the protection of the data subject or of the rights and freedoms of others could be interpreted as the rights and freedoms of the EU institution or body. According to the DPOs, this could be used to protect internal advice. In the evaluator's opinion, this exception does not cover the rights and freedoms of EU institutions and bodies. This exception relates to the balance that should be struck between the right to data protection and other fundamental rights. **Recommendations** The scope of Article 20 could be further extended, notably to the

[28] Article 20 can be broadly interpreted since Article 13 (1) (d) of Directive 95/46 also refers to "breaches of ethics for regulated professions".

ARTICLE BY ARTICLE ANALYSIS		
		following situations: ▶ Article 20 (1) (a) concerning "the prevention, investigation, detection and prosecution of criminal offences" could be extended to administrative investigations and disciplinary measures; ▶ The exceptions pertaining to Article 20 (1) (b) and (d) could also be amended to handle practical difficulties (such as the necessity of derogating data protection principles for specific security reasons); ▶ In the context of telecommunication, the exceptions provided for by Article 20 could be extended to Articles 36, 37.2 and 38. In this regard, please refer to the *case study dedicated to coherence between Regulation (EC) No 45/2001 and the ePrivacy Directive*.
Section 7 CONFIDENTIALITY AND SECURITY OF PROCESSING		
Article 21 Confidentiality of processing	A person employed with a Community institution or body and any Community institution or body itself acting as processor, with access to personal data, shall not process them except on instructions from the controller, unless required to do so by national or Community law.	**Implementation and application** ▶ ArticlesArticle 21 and 23 are implemented and applied by a large majority of EU institutions and bodies. ▶ The wording of Article 21 raises interpretation issues and is not adequate for addressing confidentiality matters: o The provision appears to target only internal data processors. o The provision could be interpreted as stating that a person employed within an EU institution or body who processes personal data under the instruction of the data controller could be considered to be a data processor.

ARTICLE BY ARTICLE ANALYSIS		
		○ The definition of a controller is unclear and inconsistent throughout the Regulation (comparison with Article 25). **Recommendation** ► Clarify the wording of Article 21 in order to avoid any inconsistencies; the evaluator recommends broadening its scope of application.
Article 22 Security of processing	1. Having regard to the state of the art and the cost of their implementation, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing. 2. Where personal data are processed by automated means, measures shall be taken as appropriate in view of the risks in particular with the aim of: (a) preventing any unauthorised person from gaining access to computer systems processing personal data; (b) preventing any unauthorised reading, copying, alteration or removal of storage media; (c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data; (d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities;	**Implementation and application** ► This articleArticle is implemented across EU institutions and bodies. It requires them to design, implement and maintain appropriate policies, procedures and systems. Levels of implementation vary. No specific pattern supporting this observation can be highlighted. ► Further, the perceived level of implementation of Article 22 can vary across the units and divisions and among the personnel within an EU institution or body. However, it should be pointed out that the EU institutions and bodies operating in a highly regulated context have effectively implemented Article 22 (such as EU LISA). ► Article 22 of the Regulation is insufficiently applied across EU institutions and bodies and the overall level of maturity appear low. This provision encompasses a (non-exhaustive) check list of control objectives and an obligation to design, implement and maintain risk management policies, procedures and systems on the basis of the state of the art (Article 22.1).Article 22 is often misunderstood by EU institutions and bodies as a mere check list. ► Risk assessment: ○ Only a third of EU institutions and bodies conduct risk

ARTICLE BY ARTICLE ANALYSIS		
	(e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers; (f) recording which personal data have been communicated, at what times and to whom; (g) ensuring that it will subsequently be possible to check which personal data have been processed, at what times and by whom; (h) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body; (i) ensuring that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation; (j) designing the organisational structure within an institution or body in such a way that it will meet the special requirements of data protection.	assessments and privacy assessments on most of personal data processing operations. ○ The others apply Article 22 insufficiently (few risk assessments, mostly performed in an *ad hoc* manner). ○ This highlights a lack of awareness and initiative on the part of certain project managers together with a lack of formalised procedures, methodologies and coordination at the organisational level. ► Logical access controls and network restrictions are among the security measures that have been implemented, according to data protection officers interviewed. ► It should also be noted that where personal data processing operations are likely to raise significant risks, certain EU institutions and bodies may use anonymisation or pseudonymisation mechanisms to mitigate the identified risks. ► The survey conducted highlighted that among the respondent EU entities, few have formally defined a process for data anonymisation and/or pseudonymisation. Nonetheless, ad-hoc processes are widely used for data anonymisation or limited data anonymisation is performed. ► Furthermore, some of these entities carry out regular risk assessments in order to accommodate new potential threats and monitor the effectiveness of the measures implemented. ► According to the DPOs and IT officers interviewed, several IT security incidents have been recorded across EU institutions and bodies in recent years. Nonetheless, very few data breach incidents putting personal data at significant risk, have been recorded. ► The EDPS has a key role in enforcing the implementation of this articleArticle. The EDPS IT policy unit regularly conducts

ARTICLE BY ARTICLE ANALYSIS		
		technical security inspections. **Recommendations** ▶ Awareness-raising is essential in order to increase the level of implementation of Article 22 within EU institutions and bodies. ▶ The DPOs of EU institutions and bodies, Local Information Security Officers and the EDPS should collaborate and organise regular workshops. ▶ Regular inspections by the EDPS should be carried out in order to raise awareness on compliance. ▶ EDPS guidance for the EU institutions and bodies could be helpful in order to shed light on the necessity of implementing a risk management approach underin respect of Article 22.
Article 23 Processing of personal data on behalf of controllers	1. Where a processing operation is carried out on its behalf, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by Article 22 and ensure compliance with those measures. 2. The carrying out of a processing operation by way of a processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: (a) the processor shall act only on instructions from the controller; (b) the obligations set out in Articles 21 and 22 shall also be incumbent on the processor unless, by virtue of Article 16 or Article 17(3), second indent, of Directive 95/46/EC, the processor is already subject to obligations with regard to confidentiality and security laid down in the national law of one of the Member States. 3. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the	**Implementation and application** ▶ ArticlesArticle 21 and 23 are implemented and applied by a large majority of EU institutions and bodies. ▶ The DG Budget had adopted standard security and confidentiality clauses that are used by a large majority of EU institutions and bodies. This clause has been reviewed by the EDPS (see report Measuring Compliance 2013). Other clauses are also used by EU institutions and bodies, notably to tackle more complex cases. **Recommendation** ▶ Ensure the broad diffusion of the DG Budget's (European Commission) template clause and other template clauses to be incorporated into SLAs.

ARTICLE BY ARTICLE ANALYSIS		
	measures referred to in Article 22 shall be in writing or in another equivalent form.	
Section 8 DATA PROTECTION OFFICER		
Article 24 Appointment and tasks of the Data Protection Officer	1. Each Community institution and Community body shall appoint at least one person as data protection officer. That person shall have the task of:	**Implementation and application** ▶ The requirement to appoint a DPO was implemented by the implementing rules adopted by each institution or body as well as by the Professional Standards for Data Protection Officers of the EU institutions and bodies adopted by the Network of Data Protection Officers. The position, tasks and duties of DPOs are described in these rules. ▶ A DPO has been appointed in all EU institutions and bodies. ▶ *See* also Article 24.4 and the Annex ▶ The range of powers appears to be adequate to allow DPOs to perform their tasks even though some DPOs wish to enhance the powers provided (e.g. by introducing the power to prohibit a data processing operation). DPO's Difficulties arise from their lack of authority (poor support from the management) or insufficient time to perform their duties.
	(a) ensuring that controllers and data subjects are informed of their rights and obligations pursuant to this Regulation;	**Informing data controllers** ▶ Informing data controllers is the most time-consuming activity. ▶ Best practices for DPOs: train the controllers, develop guidelines, develop IT tools, attend management meetings on a regular basis, etc. **Informing data subjects** ▶ Informing data subjects is the third most important activity performed by DPOs in terms of time spent. It is mainly carried

ARTICLE BY ARTICLE ANALYSIS		
		out by drafting information notices. ► The number of requests from data subjects is very low because of poor awareness among data subjects.
	(b) responding to requests from the European Data Protection Supervisor and, within the sphere of his or her competence, cooperating with the European Data Protection Supervisor at the latter's request or on his or her own initiative;	**Implementation and application** ► This is the second most time-consuming activity for DPOs. ► The balance between the duty to cooperate with the EDPS and the duty of confidentiality (Article 339 TFUE) may be hard to achieve in practice. DPOs are in a delicate position; they need to earn the trust of their management to effectively perform their duties and at the same time collaborate with the EDPS.
	(c) ensuring in an independent manner the internal application of the provisions of this Regulation;	**Implementation and application** ► The DPO must provide the appointing institution/body with recommendations and advice on the application of data protection provisions. ► This paragraph is applied by the DPO to oversee application of the Regulation: o To ensure compliance within his or her institution although he/she does not have any concrete enforcement power over controllers. o To investigate on his or her own initiative or at the request of the institution/body (few inquiries are carried out by the DPOs).
	(d) keeping a register of the processing operations carried out by the controller, containing the items of information referred to in Article 25(2);	► *See* Article 26.

ARTICLE BY ARTICLE ANALYSIS		
	(e) notifying the European Data Protection Supervisor of the processing operations likely to present specific risks within the meaning of Article 27. That person shall thus ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.	**Implementation and application** ▶ Performing prior checking is excessively burdensome for DPOs. **Recommendation** ▶ It could be envisaged to reduce the scope of prior checking and put the emphasis on a"*risk-based approach*" and/or the "responsibility and accountability" principle.
	2. The Data Protection Officer shall be selected on the basis of his or her personal and professional qualities and, in particular, his or her expert knowledge of data protection.	**Implementation and application** ▶ The selection procedure is effectively implemented and applied, as there is a DPO appointed in all EU institutions and bodies. The DPOs gain data protection experience and knowledge after their appointment. ▶ The survey shows that 33% of the DPO respondents stated that they did not have any background in data protection before taking their position as a DPO. **Recommendation** ▶ Development of a "newcomers' training toolkit", available online, for newly appointed DPOs. ▶ In order to foster DPO independence, it could be envisaged to allow smaller institutions to jointly appoint a DPO, similar to the possibility to set up common Joint Committees and common disciplinary boards (see Articles 9(1a) of the Staff Regulations and 5(1) of Annex IX to the Staff Regulations).

ARTICLE BY ARTICLE ANALYSIS		
	3. The selection of the Data Protection Officer shall not be liable to result in a conflict of interests between his or her duty as Data Protection Officer and any other official duties, in particular in relation to the application of the provisions of this Regulation.	See Article 24.7.
	4. The Data Protection Officer shall be appointed for a term of between two and five years. He or she shall be eligible for reappointment up to a maximum total term of ten years. He or she may be dismissed from the post of Data Protection Officer by the Community institution or body which appointed him or her only with the consent of the European Data Protection Supervisor, if he or she no longer fulfils the conditions required for the performance of his or her duties.	**Implementation and application (together with Article 24.1)** ▶ The obligation to appoint a DPO was implemented (see implementing rules of each institution or body and Professional Standards for DPOs of the Network of DPOs of the EU institutions and bodies). ▶ A DPO has been appointed in all EU institutions and bodies. ▶ DPOs are appointed for a term of between two and five years, eligible for reappointment up to a maximum total term of ten years. This term may raise practical difficulties as it takes several years for DPOs to gain experience on data protection matters (notably in the case of part-time DPOs). By the time the DPOs reach an adequate level of knowledge, they have to leave their functions. In practice, there are some institutions and bodies where the previous DPO still acts as *de facto* DPO. **Recommendation** ▶ The length of this appointment could be made non mandatory.
	5. After his or her appointment the Data Protection Officer shall be registered with the European Data Protection Supervisor by the institution or body which appointed him or her.	▶ The appointment is notified to the EDPS.
	6. The Community institution or body which appointed the Data Protection Officer shall provide him or her with the staff and resources necessary to carry out his or her duties.	**Implementation and application** • **Concerning DPOs** ▶ Most DPOs work part-time: only 12% of the DPO respondents work full time on data protection matters within their

ARTICLE BY ARTICLE ANALYSIS		
		institution. They are assisted by (on average) 0.35 FTEs in carrying out their duties (see evaluation question on efficiency). ▶ DPO activities require a specific expertise and time to properly conduct the tasks (see the recommendations in the Annex). ▶ Approximately 50% of DPOs struggle to complete their tasks in a timely manner. ▶ The EDPS underlines the importance of appointing a full-time DPO in the largest institutions and in smaller institutions in order to disseminate a data protection culture and establish relevant tools. ▶ Certain DPOs would favour the future Regulation including deputy or assistant DPOs and a data protection office in order to reinforce their authority. This option should be counterbalanced with the inconvenience of adding an additional level of authority which will bring more complexity to data protection governance. • **Concerning networks of DPCs** ▶ Networks of DPCs have emerged in large-scale institutions. The question of the opportunity to add an explicit reference to the role of DPC can be discussed. Certain DPOs and DPCs would favour the future Regulation laying down the function of the DPC which would allow them to better assert their authority within the institution. As stated previously, this option should be counterbalanced with the inconvenience of adding an additional level of authority which will bring more complexity to data protection governance.

ARTICLE BY ARTICLE ANALYSIS		
	7. With respect to the performance of his or her duties, the Data Protection Officer may not receive any instructions.	**Implementation and application** ▶ The document on professional standards for DPOs from the DPO network sets out a list of best practices to help ensure the independence of the DPO. ▶ The independence of the DPO seems to be closely linked to the position of the DPO within the hierarchy and the support management provides to his or her function. ▶ Only 24% of the DPO respondents say that their position allows them to exercise their functions in total independence. Respondents to the survey provided several reasons for this. ▶ When DPOs report directly to the highest level of management (e.g. the Executive Director) who supports his or her actions, it fosters the independence and the authority of the DPO in relation to his or her colleagues. ▶ Independence could be weakened where DPOs are part-time and act as a data controller or perform other duties such as providing legal advice. In addition, this can place DPOs in situation where a conflict of interest arises.

ARTICLE BY ARTICLE ANALYSIS		
	8. Further implementing rules concerning the Data Protection Officer shall be adopted by each Community institution or body in accordance with the provisions in the Annex. The implementing rules shall in particular concern the tasks, duties and powers of the Data Protection Officer. *Recital 32: In each Community institution or body one or more Data Protection Officers should ensure that the provisions of this Regulation are applied and should advise controllers on fulfilling their obligations.*	**Implementation and application** ▶ Article 24.8 is implemented by the EDPS guidelines relating to the "implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8)".[29] In this paper, the EDPS also recommends adding rules relating to the role of the controllers and rules whereby data subjects may exercise their rights. These guidelines detail the information that should be enshrined in these implementing rules (e.g. the tasks, duties and powers of the DPO). The draft implementing rules are submitted to the EDPS for consultation. ▶ The implementing rules are generally adopted or submitted to the EDPS for consultation in the year of or the year after the establishment of the EU body.[30] ▶ Pursuant to the bi-annual survey conducted by the EDPS in 2013[31], almost all EU institutions have adopted implementing rules or are in the process of adopting these rules, except the EUISS.

[29] https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-07-29_Guidelines_DPO_tasks_EN.pdf.
[30] See https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2014/14-01-24_survey_report_EN.pdf.
[31] See https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2014/14-01-24_survey_report_EN.pdf.

ARTICLE BY ARTICLE ANALYSIS		
Article 25 Notification to the Data Protection Officer	1. The controller shall give **prior notice to the Data Protection Officer** of any processing operation or set of such operations intended to serve a single purpose or several related purposes. 2. The information to be given shall include: (a) the name and address of the controller and an indication of the organisational parts of an institution or body entrusted with the processing of personal data for a particular purpose; (b) the purpose or purposes of the processing; (c) a description of the category or categories of data subjects and of the data or categories of data relating to them; (d) the legal basis of the processing operation for which the data are intended; (e) the recipients or categories of recipient to whom the data might be disclosed; (f) a general indication of the time limits for blocking and erasure of the different categories of data; (g) proposed transfers of data to third countries or international organisations; (h) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 22 to ensure security of processing. 3. Any change affecting information referred to in paragraph 2 shall be notified promptly to the Data Protection Officer.	**Implementation and application** • **Concerning the obligation to notify data processing operations** ▶ The obligation to notify data processing operations is largely implemented and applied by EU institutions and bodies. ▶ This obligation falls to data controllers even though they often rely on the DPOs to complete the notification forms. ▶ Notifications are often performed after the processing operations, mostly because data controllers do not complete notifications or notify the DPO *ex post*. ▶ Over time, notification become an essential tool for promoting compliance but has also created a significant burden. ▶ DPOs and data controllers emphasised the need for "real compliance" rather than spending time on the drafting of notifications. ▶ Some questions have been raised as to what needs to be notified (in particular, do agencies need to notify certain IT applications already notified by the European Commission?). • **Concerning the obligation to keep a register of data processing operations** ▶ The obligation to keep a register of data processing operations is applied in all EU institutions and bodies surveyed, although the register is not regularly updated. ▶ The DPO must keep a register which must be made available to the public via the EDPS. ▶ Some EU institutions and bodies also keep an inventory of the data processing operations. ▶ It has been pointed out that in order to formalize a practice already applied, it could be stipulated that notifications be validated by the DPO in order to be added to the register.
Article 26 Register	A register of processing operations notified in accordance with Article 25 shall be kept by each Data Protection Officer. The registers shall contain at least the information referred to in Article 25(2)(a) to (g). The registers may be inspected by any person directly or indirectly through the European Data Processing Supervisor. (24) The necessary technical measures should be adopted to allow access to the registers of processing operations carried out by Data Protection Officers through the independent supervisory authority.	

ARTICLE BY ARTICLE ANALYSIS		
		Recommendations ► Because a level of maturity regarding data protection issues has been reached in a large majority of EU institutions and bodies, the administrative burden created by the notification of data processing operations could be reduced. Possible changes include: o Abolishing the notification system: this presents significant risks of decreasing the level of data protection compliance but a requirement for DPOs to keep an inventory instead of a register could be introduced. o Limiting the scope of notifications to risky operations: the main difficulty would be to set the threshold and raise data controllers' awareness of data protection issues. o Reducing the range of information required by Article 25.2: simplification of notifications but risk of reducing the quality of the notification and reducing the level of compliance. ► Improving data privacy IT management tools used for notifications.
Section 9 PRIOR CHECKING BY THE EUROPEAN DATA PROTECTION SUPERVISOR AND OBLIGATION TO COOPERATE		
Article 27 **Prior checking**	1. 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 shall be subject to prior checking by the European Data Protection Supervisor. 2. The following processing operations are likely to present such risks: (a) processing of data relating to health and to suspected offences, offences, criminal convictions or security measures; (b) processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct; (c) processing operations allowing linkages not provided for pursuant to national or	► The wording of Article 27 is unclear with regard to whether the list enshrined in paragraph 2 is exhaustive (in the light of Article 27.5). **Implementation and application (together with Article 46(j))** ► Processes/procedures have been adopted in a majority of EU institutions and bodies. Moreover, Articles 19 to 23 of the EDPS Rules of procedure and the EDPS position paper on "Monitoring and Ensuring Compliance with Regulation (EC) No 45/2001, 13 December 2010" relate to the obligation to carry out prior checking.

ARTICLE BY ARTICLE ANALYSIS		
	Community legislation between data processed for different purposes; (d) processing operations for the purpose of excluding individuals from a right, benefit or contract. 3. The prior checks shall be carried out by the European Data Protection Supervisor following receipt of a notification from the Data Protection Officer who, in case of doubt as to the need for prior checking, shall consult the European Data Protection Supervisor. 4. The European Data Protection Supervisor shall deliver his or her opinion within two months following receipt of the notification. This period may be suspended until the European Data Protection Supervisor has obtained any further information that he or she may have requested. When the complexity of the matter so requires, this period may also be extended for a further two months, by decision of the European Data Protection Supervisor. This decision shall be notified to the controller prior to expiry of the initial two-month period. If the opinion has not been delivered by the end of the two-month period, or any extension thereof, it shall be deemed to be favourable. If the opinion of the European Data Protection Supervisor is that the notified processing may involve a breach of any provision of this Regulation, he or she shall where appropriate make proposals to avoid such breach. Where the controller does not modify the processing operation accordingly, the European Data Protection Supervisor may exercise the powers granted to him or her under Article 47(1). 5. The European Data Protection Supervisor shall keep a register of all processing operations that have been notified to him or her pursuant to paragraph 2. The register shall contain the information referred to in Article 25 and shall be open to public inspection.	▶ EDPS carries out prior checking on all notifications sent by DPOs and is also consulted in case of doubt as to the need for prior checking. ▶ In practice, most processing submitted for prior checking falls within the scope of Article 27.2 of Regulation (EC) No 45/2001. However, there are some exceptions, such as processing operations relating to cloud computing and RFID that are also submitted for prior checking. It should be underlined that these operations are technologies/tools and not processing purposes as such. The fact that a new technology could raise significant security-related risks is not a sufficient criterion in itself to be subject to prior checking. However, a change in technology that dramatically increases risks to rights and freedoms will be subject to prior checking. When necessary, these technologies/tools are therefore linked to one of the operations set forth in Article 27. ▶ The EDPS pointed out that there is an issue of translation in Article 27.2 as *"mesures de suretés"* were translated by "security measures". ▶ Article 27 2 (a), (b) and (d) are referred to on a regular basis. Article 27.2. (c) is rarely used (one prior check performed). ▶ The EDPS has narrowed the scope of application of Article 27. 2 (a) relating *inter alia* to health data by stating that the processing of health data must play a key role. ▶ The findings of the EDPS are enshrined in prior check opinions which are presented to the data controller and/or to the DPO of the institution or body concerned. ▶ The opinion of the EDPS should be delivered prior to the start of the data processing operation ("*ex ante* prior check"). However, since some processing operations were carried out before the appointment of the EDPS, the Supervisor also carries out prior checking afterwards ("*ex post* prior check").

ARTICLE BY ARTICLE ANALYSIS		
		▶ The EDPS should deliver its opinion within two months but considers that it is not bound by this deadline when the notification arrives after the start of the processing operation. This practice has raised criticism from DPOs who, in practice, need to wait for long periods before being provided with the opinion. ▶ The EDPS follows up the opinions even though it is not expressly provided for by Regulation (EC) No 45/2001. This appears to be an efficient means to enhance long-term compliance. ▶ Prior checks previously represented 70% of EDPS staff dedicated to supervisory activity. The EDPS' efficiency in performing prior checks has increased over time: ▶ The EDPS has gained maturity with regard to monitoring the application of the Regulation; ▶ Starting in 2010 the EDPS adopted thematic guidelines in order to facilitate the processing of prior check notifications; ▶ The EDPS has narrowed down the scope of application of prior checking and has simplified the opinion submitted after prior check, focusing on specific compliance issues (it now addresses only non-compliance issues); ▶ Following up on the recommendations made in opinions allows the EDPS to take stock of its previous experience and to build its guidelines; ▶ Most of the vast backlog of *ex-post* prior checking processing operations has been notified to the EDPS. ▶ There are still some drawbacks: ▶ The scope of application of Article 27 (1) and (2) appears to be unclear for some EU institutions and bodies. A significant number of prior checking notifications are not admissible but the EDPS needs to instruct the notification received to reach this conclusion. ▶ Furthermore, criticism has been raised **concerning the opinion timeframes and their failure to reflect operational needs.**

ARTICLE BY ARTICLE ANALYSIS		
		▶ Prior checking is highly burdensome for DPOs. **Recommendations (together with Article 46(j))** ▶ Article 27 and 46 (j) of Regulation (EC) No 45/2001 are effectively implemented and applied. However, some further improvements could be considered: o It is necessary to increase communication on prior checking. Prior checking should only be considered as one aspect of compliance. o Further clarification of the scope of prior checking could help to reduce unfounded notifications. o Further to the adoption of guidelines (see below), a dialogue should be engaged with EU institutions and bodies to reduce the administrative burden linked to prior checking. o The implementation of Regulation (EC) No 45/2001 should be further improved by the upcoming publication of prior check guidelines. ▶ Prior checking is a **relevant mechanism** to protect the personal data and privacy of individuals in the context of risky operations. Improvements should nevertheless be planned in order to reduce the burden they create. Some stakeholders favour the introduction of a system of block exemptions in line with the current practices of adopting guidelines to ease the prior checking process. Nevertheless, it may be advisable to narrow the scope of prior checking to the core risky operations.
Article 28	1. The Community institutions and bodies shall inform the European Data	**Implementation and application (together with Article 46)**

ARTICLE BY ARTICLE ANALYSIS		
Consultation	Protection Supervisor when drawing up administrative measures relating to the processing of personal data involving a Community institution or body alone or jointly with others.	▶ Article 28 (1) is effectively implemented by the EDPS Rules of Procedure (section 3) and the Policy on Consultations in the field of Supervision and Enforcement. This provision has been interpreted and applied by the EDPS as an EDPS obligation to supervise the consultation performed by the DPOs. Indeed, although the EDPS encourages institutions and bodies to inform and consult the EDPS, the EDPS advises data controllers to consult their DPO as a first step. The matter can be submitted to the EDPS for consultation thereafter in cases of complexity or for subjects concerning appreciable risks to the rights and freedoms of the data subjects. **Effectiveness has increased through the building of guidelines by the EDPS and the reduction of the workload.** ▶ Institutions and bodies inform the EDPS when they take administrative measures such as implementing rules concerning DPOs (Article 24.8 of Regulation (EC) No 45/2001) and internal administrative rules relating to the processing of personal data (e.g. use of e-mail, e-monitoring, archiving, etc.) to permit the EDPS to provide any advice that might be deemed necessary. In this regard, the EDPS may adopt opinions on administrative measures related to data protection adopted by European institutions and bodies. ▶ The wording of Article 28.1 has been under discussion. The DPO network pointed out that Article 28.1 should say "consult" instead of "inform" as the obligation relates to the heading on "Consultations" within the Regulation. In this regard, the term "inform" seems closer to the practices of the EDPS acting to oversee the work performed by the DPOs and therefore, more appropriate than the term "consult". Stakeholders have underlined that the relationship between Article 28(1) and the prior checking mechanism may be

ARTICLE BY ARTICLE ANALYSIS		
		unclear as the EDPS does not seem to accept Article 28(1) consultations where a subsequent prior checking will be necessary.
	2. When it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, the Commission shall consult the European Data Protection Supervisor.	**NB:** the EDPS also provides legal advice to EU institutions and bodies on the basis of Article 41(2). **Implementation and Application** ▶ This obligation is implemented by the EDPS Rules of Procedure and the Policy Paper on Consultation of June 2014[32], which interpret and provide a detailed procedure for legislative consultation. The EDPS policy paper on consultation of June 2014 aims at interpreting its role with regard to legislative consultation and in particular, in terms of limitations in scope, working methods and main orientations. ▶ The EDPS has developed a 'policy toolkit' – which includes general guidance to the legislator, for instance through thematic or sectorial guidelines – in order to raise awareness of institutions on data protection and privacy impacts. A memorandum of understanding with the three main institutions (European Parliament, Council of the European Union, and European Commission) is also envisaged by the EDPS. ▶ **Article 28.2 does neither specify the exact time for consultation nor the legislative instruments subject to consultation.** According to the EDPS, the consultation covers a wide range of acts: legislative texts, but also other legal documents which are part of the legislative process

[32] Policy Paper "The EDPS as an advisor to EU institution on Policy and Legislation: building on 10 years of experience", June 2014.

ARTICLE BY ARTICLE ANALYSIS		
		(implementing acts, delegated acts, green papers, etc.). ▶ **This obligation is thoroughly applied by the EDPS.** Each year, the EDPS identifies the legislative and policy making proposals with the most impact for data protection on the basis of the European Commission's work program. A meeting is organized in December when the European Commission has set the work program. In its policy inventory the EDPS lists the policy initiatives planned by the European Commission that it will comment upon or monitor. The EDPS provides advice to the legislator at all stages of the legislative process, from the Commission's draft to the definitive adoption of the text. ▶ **There are different stages and instruments of consultations:** 1. According to Article 28.2 of the EDPS Rules of Procedure, formal legislative opinions are the main instruments used by the EDPS; they are issued in respect of proposals adopted by the Commission and include a full review of data protection related aspects of the proposal or other instrument. They analyse the impact of the text with regard to data protection and privacy. As a rule, the EDPS issues opinions on non-legislative texts only if data protection is a core element.[33] 2. Occasionally, formal comments are drafted on specific data protection issues. 3. Informal comments on the Commission's drafts for legislative proposals on which EDPS must in theory be consulted by the Commission. The informal comments are confidential and they often precede formal consultation.

[33] EDPS Annual Report 2013.

ARTICLE BY ARTICLE ANALYSIS		
		These informal comments make it possible to take data protection requirements into consideration at an early stage. ▶ The EDPS' activity in advising the European Commission on the legislative process has increased significantly in recent years. ▶ Informal comments allow for early integration of data protection measures into the process, and this timing appears to be more effective in terms of taking data protection into account in the final proposal. ▶ The consultation of the EDPS by other institutions (European Parliament and Council of the European Union) in the course of the legislative process is not provided for in the Regulation, although the EDPS has regular contacts with these institutions as described in more detail in the section dedicated to the EDPS. ▶ Relations with the European Parliament are satisfactory. With regard to the relationship with the Council, the EDPS must wait for official invitations to attend Council meetings, which are only provided if the EDPS is expected to make a presentation. In order to change this situation, the EDPS emphasizes that the EDPS should have a recognized status in relation to the Council. The issue of this status is part of the draft Memorandum. However, it should be stressed that the Council has repeatedly invited the EDPS to participate in meetings and discussions even though it has no obligation to do so pursuant to Regulation (EC) No 45/2001 and the Treaties. ▶ The section dedicated to the EDPS' contribution to providing opinions on the legislative process impacting personal data is very limited in the Regulation. This task has reached a

ARTICLE BY ARTICLE ANALYSIS		
		satisfactory level of maturity thanks to the implementing rules set up by the EDPS and constructive cooperation with the European Commission. Several hurdles still need to be cleared, starting with a clarification of the process in the Regulation, to foster the effectiveness of the support offered by the EDPS to the legislative process. **Recommendations** There are two available options to increase the effectiveness of the consultation obligation: ▶ **Hard Law:** amendment of Regulation (EC) No 45/2001. Article 28.2 of Regulation (EC) No 45/2001 could be amended to specify the consultation process and the types of texts subject to consultation. Informal consultations should be formalized. ▶ **Soft Law:** drafting of a Memorandum of Understanding. Indeed, an alternative option would be adopt a memorandum of understanding between the three legislative institutions (European Commission, Council of the European Union and European Parliament) and the EDPS.
Article 29 Obligation to provide information	The Community institutions and bodies shall inform the European Data Protection Supervisor of the measures taken further to his or her decisions or authorisations as referred to in Article 46(h).	**Implementation and application** ▶ The evaluator is not aware of specific procedures/processes/internal rules pertaining to these specific obligations. ▶ These obligations are applied by a large majority of EU institutions and bodies consulted. ▶ EU institutions and bodies are cooperative and reactive in the course of investigations by the EDPS. Nevertheless, delays in

ARTICLE BY ARTICLE ANALYSIS		
		responding to the EDPS have been pointed out. ► In some EU institutions and bodies, DPOs are likely to carry out these obligations instead of data controllers. ► DPOs are not systematically informed of the exchange of information between the EDPS and the data controller.
Article 30 Obligation to cooperate	At his or her request, controllers shall assist the European Data Protection Supervisor in the performance of his or her duties, in particular by providing the information referred to in Article 47(2)(a) and by granting access as provided in Article 47(2)(b).	See Article 29.
Article 31 Obligation to react to allegations	In response to the European Data Protection Supervisor's exercise of his or her powers under Article 47(1) (b), the controller concerned shall inform the Supervisor of its views within a reasonable period to be specified by the Supervisor. The reply shall also include a description of the measures taken, if any, in response to the remarks of the European Data Protection Supervisor.	See Article 29.
Chapter III REMEDIES		
Article 32 Remedies	1. The Court of Justice of the European Communities shall have jurisdiction to hear all disputes which relate to the provisions of this Regulation, including claims for damages. 2. Without prejudice to any judicial remedy, every data subject may lodge a complaint with the European Data Protection Supervisor if he or she considers that his or her rights under Article 286 of the Treaty have been infringed as a result of the processing of his or her personal data by a Community institution or body. In the absence of a response by the European Data Protection Supervisor within six months, the complaint shall be deemed to have been rejected.	► The EDPS has the duty to hear and investigate complaints. The EDPS makes the distinction between complaints lodged by individuals (Article 32) and complaints by EU staff (Article 33). While any individual may complain to the EDPS about an alleged violation of his or her rights to the protection of his or her personal data, it should be pointed out that EU staff may bring a complaint about any alleged violation of data protection rules, whether he or she is directly affected or not. See also Article 46 (a) and (b). ► The following sanctions may be imposed by the EDPS: (i) warn or admonish the controller (Article 47 (d)), (ii) impose a temporary or

ARTICLE BY ARTICLE ANALYSIS		
	3. Actions against decisions of the European Data Protection Supervisor shall be brought before the Court of Justice of the European Communities. 4. Any person who has suffered damage because of an unlawful processing operation or any action incompatible with this Regulation shall have the right to have the damage made good in accordance with Article 288 of the Treaty. Recital (31) Liability arising from any breach of this Regulation is governed by the second paragraph of Article 288 of the Treaty.	definitive ban on processing (Article 47 (f), (iii) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission (Article 47 (g), (iv) refer the matter to the Court of Justice of the European Union (Article 47 (h)), (v) intervene in actions brought before the Court of Justice of the European Union (Article 47 (i)). ► Although DPOs do not have the power to impose sanctions on data controllers, they are responsible for ensuring the internal application of the provisions of the Regulation. Therefore, DPOs may hear and investigate complaints (at the outset). **Implementation and application** (together with Article 33 and 46 (a) and (b)) ► The number of complaints made to DPOs and the EDPS is not significant and could indicate a lack of awareness on data protection. ► Feedback from data subjects indicates that the data controller does not always reply to their complaints (when the matter is referred to him or her). ► The decision of the EDPS on complaints may be subject to review. It should be noted that any interested party can ask the EDPS for a review its decision. The EDPS stated that of 32 review requests, only one had sufficient grounds. The review must be lodged within one month of the date of receipt of the decision. Concerned parties may also directly challenge the decision before the Court of Justice of the European Union in accordance with Article 263 of the TFEU.[34]

[34] See CJEU, Order of the General Court, 19 February 2011, Erasmia Kitou v EDPS, T-164/09.

ARTICLE BY ARTICLE ANALYSIS		
Article 33 Complaints by Community staff	Any person employed with a Community institution or body may lodge a complaint with the European Data Protection Supervisor regarding an alleged breach of the provisions of this Regulation governing the processing of personal data, without acting through official channels. No-one shall suffer prejudice on account of a complaint lodged with the European Data Protection Supervisor alleging a breach of the provisions governing the processing of personal data.	**Implementation and application** ► The Court of Justice of the European Union has already sanctioned an EU institution for data protection breaches.[35] ► The argument pertaining to the infringement of the provisions of Regulation (EC) No 45/2001 has been brought in several cases before the Court of Justice.[36] For example, the unlawful disclosure of the name of an official subject to disciplinary proceedings by the European Commission is an infringement of the provisions of Regulation (EC) No 45/2001.[37] ► There are several cases where the CJUE awarded damages to an EU official (See for example, *Nanopoulos v Commission*[38], *Commission of the European Communities v Augusto Brazzelli Lualdi and others*[39] and *Commission of the European Communities v Marie-Claude Girardot* [40]).
Chapter IV PROTECTION OF PERSONAL DATA AND PRIVACY IN THE CONTEXT OF INTERNAL TELECOMMUNICATIONS NETWORKS		
Article 34 Scope	Without prejudice to the other provisions of this Regulation, this Chapter shall apply to the processing of personal data in connection with the use of telecommunications networks or terminal equipment operated under the control of a Community institution or body. For the purposes of this Chapter, 'user' shall mean any natural person	**Preliminary remarks** ► *Given the stakeholders consulted, it is difficult to assess how Chapter IV of Regulation (EC) No 45/2001 was implemented and applied throughout EU Institutions and bodies. Nevertheless, it is important to underline that this chapter is*

[35] CJEU, European Union Civil Service Tribunal, 5 July 2011, V. v European Parliament, Case F-46/09; CJEU, 11 May 2010, Fotios Nanopoulos v European Commission, Case F-30/08 and confirmed on appeal T-308/10 P.

[36] See for example, CJEU, 16 September 2009, Fiorella Vinci v European Central Bank, Case F-130/07.

[37] CJEU, 11 May 2010, Fotios Nanopoulos v European Commission, Case F-30/08 (paragraph 171).

[38] CJEU, 11 May 2010, Fotios Nanopoulos v European Commission, Case F-30/08 and confirmed on appeal T-308/10 P.

[39] CJEC, 1 June 1994, Commission of the European Communities v Augusto Brazzelli Lualdi and others, Case C-136/92 P .

[40] CJEC, 21 February 2008, Commission of the European Communities v Marie-Claude Girardot, Case C-348/06 P.

ARTICLE BY ARTICLE ANALYSIS		
	using a telecommunications network or terminal equipment operated under the control of a Community institution or body. **Recitals:** *(10) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(5) specifies and adds to Directive 95/46/EC with respect to the processing of personal data in the telecommunications sector.* *(30) It may be necessary to monitor the computer networks operated under the control of the Community institutions and bodies for the purposes of prevention of unauthorised use. The European Data Protection Supervisor should determine whether and under what conditions that is possible.*	*now outdated insofar as it was based on the first version of the ePrivacy Directive which was updated in 2002 and 2009.* [41] *In this regard, it should be noted that the European Commission has already implemented and applied the provisions relating to the use of cookies. Given the **principle of technological neutrality**, the scope and the wording of the Regulation must sufficiently broad to encompass all current and future telecommunication technologies.* ► *Raising awareness is essential in order **to increase the level of implementation of Article 35** within EU institutions and bodies (i.e. organization of regular workshops, regular inspections to be carried out in order to raise awareness on compliance).* **Implementation and application of Chapter IV** ► The level of implementation of Chapter IV could be further improved. Only 46% of the EU institutions and bodies consulted have adopted specific procedures/processes or internal rules specific to the telecommunications sector. Nevertheless, it should be noted that the security rules provided for in this chapter should be read in the light of Article 22 on the security of data processing operations. ► **The EDPS is preparing guidelines on the processing of personal data relating to electronic communications by**

[41] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201 of 31.7.2002, p.37).
And Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' right relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ L 337 of 18.12.2009, p.11).

ARTICLE BY ARTICLE ANALYSIS		
		European Union institutions and bodies.
Article 35 Security	1. The Community institutions and bodies shall take appropriate technical and organisational measures to safeguard the secure use of the telecommunications networks and terminal equipment, if necessary in conjunction with the providers of publicly available telecommunications services or the providers of public telecommunications networks. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. 2. In the event of any particular risk of a breach of the security of the network and terminal equipment, the Community institution or body concerned shall inform users of the existence of that risk and of any possible remedies and alternative means of communication.	**Implementation and application** ► The provisions of Article 35 of Regulation (EC) No 45/2001 are similar to those of Article 22. According to the interviews performed, there is no need to include a specific body of rules pertaining to the telecommunications sector. ► The EU entities must also properly implement the necessary alert mechanisms i to ensure notification of telecommunications users in the event of any risks arising from a security breach. Several EU institutions and bodies have already implemented an obligation to notify personal data breaches to their DPO and the data subject concerned. ► In addition, EU institutions and bodies are currently faced with a growing number of attacks targeting their telecommunication networks and equipment. EU entities that have insufficiently applied Articles 35 and 22 are struggling to maintain an appropriate level of security in the face of these attacks.
Article 36 Confidentiality of communications	Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law. (19) The Community institutions and bodies should inform the competent authorities in the Member States when they consider that communications on their telecommunications networks should be intercepted, in keeping with the national provisions applicable.	**Implementation and application** ► The implementation and application of Article 36 require that the EU institutions and bodies incorporate the proper technical and organisational mechanisms to safeguard the confidentiality of communications. EU institutions and bodies may need to intercept or oversee communications and related traffic data. They may need to record calls to certain helplines, security or emergency lines or switchboards aimed

ARTICLE BY ARTICLE ANALYSIS		
		at a large number of users in order, for example, to be able to verify the content of the communication afterwards, to retain evidence, to use as a training aid, etc. ▶ The notion of "general principles of Community law" has raised interpretation issues.
Article 37 Traffic and billing data	1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection. 2. If necessary, traffic data as indicated in a list agreed by the European Data Protection Supervisor may be processed for the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications systems. These data shall be erased or made anonymous as soon as possible and no later than six months after collection, unless they need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before a court. 3. Processing of traffic and billing data shall only be carried out by persons handling billing, traffic or budget management. 4. Users of the telecommunication networks shall have the right to receive non-itemised bills or other records of calls made.	**Implementation and application** ▶ According to the principle enshrined in Article 37, traffic data should be erased or made anonymous immediately after being processed and stored for the duration necessary to transmit communications (Article 37.1). ▶ Article 37.2 provides for an exception relating to the processing of traffic data which is necessary for budget and traffic management. These data are indicated in a list subject to agreement by the EDPS, but the EDPS has stated that the list has never been published. These data may be kept for a period of six months and should then be erased or made anonymous (Article 37.2). ▶ In practice, this traffic data may be relevant in the course of the investigation of criminal offences, administrative enquiries or disciplinary proceedings. Therefore, Article 20.1 is applicable to Article 37.1, meaning that, as an exception, for specific purposes, after the establishment of calls and other connections, instead of being immediately erased or made anonymous, traffic data may be processed and stored. ▶ Article 20.1 should also cover Article 37.2. Indeed, should Article 20.1 only cover Article 37.1, it would be applicable to data which has already been erased or anonymised at the time of the investigation (insofar as Article 37.1 provides for immediate erasure or anonymisation).

ARTICLE BY ARTICLE ANALYSIS		
		▶ A practical difficulty of application lies in the technical feasibility of definitively erasing or anonymizing traffic data in communication networks which were not all designed to offer this possibility. The six-month deadline is difficult to meet in practice.
Article 38 Directories of users	1. Personal data contained in printed or electronic directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory. 2. The Community institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories, regardless of whether they are accessible to the public or not, from being used for direct marketing purposes.	**Application** ▶ On the basis of the interviews performed for the European Commission, two kinds of directories exist. There are public directories with minimum information about staff members (such as name and function) and internal directories which contain additional information only accessible within EU institutions and bodies. The public directories of the European Commission are directly accessible on the internet.
Article 39 Presentation and restriction of calling and connected line identification	1. Where presentation of calling-line identification is offered, the calling user shall have the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line identification. 2. Where presentation of calling-line identification is offered, the called user shall have the possibility via a simple means, free of charge, to prevent the presentation of the calling-line identification of incoming calls. 3. Where presentation of connected-line identification is offered, the called user shall have the possibility via a simple means, free of charge, to eliminate the presentation of the connected-line identification to the calling user. 4. Where presentation of calling or connected-line identification is offered, the Community institutions and bodies shall inform the users thereof and of the possibilities set out in paragraphs 1, 2 and 3.	**Implementation and application** ▶ The provisions relating to the presentation and restriction of calling- and connected-line identification are irrelevant and outdated, notably in the light of BYOD (Bring Your Own Device) and mobile telephones.
Article 40	Community institutions and bodies shall ensure that there are transparent procedures governing the way in which they may override	***See Article 39.***

ARTICLE BY ARTICLE ANALYSIS		
Derogations	the elimination of the presentation of calling-line identification: (a) on a temporary basis, upon application of a user requesting the tracing of malicious or nuisance calls; (b) on a per-line basis for organisational entities dealing with emergency calls, for the purpose of answering such calls.	
Chapter V INDEPENDENT SUPERVISORY AUTHORITY: THE EUROPEAN DATA PROTECTION SUPERVISOR		
Article 41 European Data Protection Supervisor	1. An independent supervisory authority is hereby established referred to as the European Data Protection Supervisor. 2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies. The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data. To these ends he or she shall fulfil the duties provided for in Article 46 and exercise the powers granted in Article 47. **Recitals:** *(3) Article 286(2) of the Treaty requires the establishment of an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies.*	**Implementation and application** ▶ The obligation to establish the EDPS and appoint the Supervisor and Assistant Supervisor was implemented according to defined procedures (see Article 42 relating to the appointment procedure). ▶ The provisions of Regulation (EC) No 45/2001 are implemented by two specific texts: the Decision of the European Data Protection Supervisor of 17 December 2012 on the adoption of Rules of Procedure and Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties ▶ Article 41 also defines the role of the EDPS.

ARTICLE BY ARTICLE ANALYSIS		
Article 42 Appointment	1. The European Parliament and the Council shall appoint by common accord the European Data Protection Supervisor for a term of five years, on the basis of a list drawn up by the Commission following a public call for candidates. An Assistant Supervisor shall be appointed in accordance with the same procedure and for the same term, who shall assist the Supervisor in all the latter's duties and act as a replacement when the Supervisor is absent or prevented from attending to them. 2. The European Data Protection Supervisor shall be chosen from persons whose independence is beyond doubt and who are acknowledged as having the experience and skills required to perform the duties of European Data Protection Supervisor, for example because they belong or have belonged to the supervisory authorities referred to in Article 28 of Directive 95/46/EC. 3. The European Data Protection Supervisor shall be eligible for reappointment. 4. Apart from normal replacement or death, the duties of the European Data Protection Supervisor shall end in the event of resignation or compulsory retirement in accordance with paragraph 5. 5. The European Data Protection Supervisor may be dismissed or deprived of his or her right to a pension or other benefits in its stead by the Court of Justice at the request of the European Parliament, the Council or the Commission, if he or she no longer fulfils the conditions required for the performance of his or her duties or if he or she is guilty of serious misconduct. 6. In the event of normal replacement or voluntary resignation, the European Data Protection Supervisor shall nevertheless remain in office	**Implementation and application** ▶ The appointment procedure is implemented and applied. The procedure is composed of two phases: o The European Commission draws up a list of candidates, following a public call for candidates. Candidates are to be selected on the basis of objective criteria as set out by Article 42.2. o The European Parliament and the Council decide on the appointment on the basis of the Commission list. ▶ However, Regulation (EC) No 45/2001 does not state any deadlines for the appointment of the EDPS and his or her Assistant. It should be emphasized that during the last appointment procedure, the appointment of the current EDPS encountered substantial delays as the appointment took more than 16 months (July 2013-December 2014). In January 2014, the European Commission considered that none of the candidates were suitable (see below). The European Commission published two new calls for candidates (one for the EDPS and one for the Assistant). In this regard, it should be noted that Article 42 does not explicitly prohibit launching two different calls for candidates. ▶ These delays raise criticism, notably concerning a lack of transparency[42]. ▶ The appointment does not raise suspicions of partiality of the EDPS; it is unlikely that the procedure would result in undue external influence. ▶ Regarding the independence of the EDPS (Article 42.2): o Article 42.5 lays down the circumstances in which

[42] See for e.g. Christopher Kuner, "The baffling case of the headless EDPS", published on https://privacyassociation.org/news/a/the-edps-mess/.

ARTICLE BY ARTICLE ANALYSIS		
	until he or she has been replaced. 7. Articles 12 to 15 and 18 of the Protocol on the Privileges and Immunities of the European Communities shall also apply to the European Data Protection Supervisor. 8. Paragraphs 2 to 7 shall apply to the Assistant Supervisor.	the EDPS may be dismissed. This is a guarantee of independence (see Commission v Hungary[43]). In *Commission v Hungary*, the Court ruled that the premature termination of the mandate of the Head of the Hungarian Supervisory Authority by a legislative change and the creation of a new supervisory authority should be considered as a lack of independence. In particular, the Court stated that the rules provided for by Article 42(4) and (5) of Regulation (EC) No 45/2001 applicable to the circumstances in which the term served by the EDPS may be prematurely brought to an end are strictly limited. These rules allow *"the EDPS to serve its full term of office, save where this is precluded for overriding and objectively verifiable reasons", and are therefore "an overarching requirement for its independence."* ○ Moreover, it should be pointed out that the fact that the EDPS is proposed by the European Commission and appointed by the Council and the European Parliament may raise independence issues insofar as all three of these EU institutions and bodies will be subject to the supervision of the EDPS. However, in light of the case law of the Court of Justice (as described below), it is unlikely that the appointment procedure would result in "external influence which would be liable to have an effect on their decisions ". Furthermore, this appointment does not appear (in practice) to raise suspicions of partiality of the EDPS

[43] CJEU, 8 April 2014, European Commission v. Hungary, Case C-288/12.

ARTICLE BY ARTICLE ANALYSIS		
		(see *Commission v Germany*, paragraph 36). **Recommendation** ▶ The appointment procedures should introduce more transparency of the selection process and follow a strict schedule in order to curtail criticism of the transparency of the procedure.
Article 43 Regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, staff and financial resources	The European Parliament, the Council and the Commission shall by common accord determine the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties and in particular his or her salary, allowances and any other benefits in lieu of remuneration. 2. **The budget authority shall ensure that the European Data Protection Supervisor is provided with the human and financial resources necessary for the performance of his or her tasks.** 3. The European Data Protection Supervisor's budget shall be shown in a separate budget heading in Section VIII of the general budget of the European Union. 4. The European Data Protection Supervisor shall be assisted by a Secretariat. The officials and the other staff members of the Secretariat shall be appointed by the European Data Protection Supervisor; their superior shall be the European Data Protection Supervisor and they shall be subject exclusively to his or her direction. Their numbers shall be decided each year as part of the budgetary procedure. 5. The officials and the other staff members of the European Data Protection Supervisor's Secretariat shall be subject to the rules and regulations applicable to officials and other servants of the European Communities. 6. In matters concerning the Secretariat staff, the European Data Protection Supervisor shall have the same status as the institutions within the meaning of Article 1 of the Staff Regulations of Officials of the European Communities.	**Implementation and Application** ▶ The human and financial resources allow the EDPS to perform its tasks. Within the EDPS, the allocation of resources per objectives assigned is balanced between supervisory and advisory activities. Both units in charge of these roles have increased their activities in recent years, without increasing the number of staff dedicated to each unit. Both units benefit from efficiency gains made over the last 5 years, although further follow-up would be helpful to help DPOs raise awareness in institutions and bodies. **Recommendation** ▶ According to our assessment, Regulation (EC) No 45/2001 places more importance on supervisory activities (Articles 41, 46 and 47) than on advisory activities (Article 28.2 and 46 (d)). However, 50% of EDPS' staff is involved in advisory activities. Part of the explanation lies in the fact that the EDPS' advisory activities extend beyond the scope of Article 28.2 and even of Regulation (EC) No 45/2001 to embrace other sources (e.g. Directive 95/46, specific regulations setting up large-scale IT systems for coordinated supervision activities, etc.). ▶ A reallocation of resources in favour of the supervision and

ARTICLE BY ARTICLE ANALYSIS		
		enforcement unit could be envisaged in order to (i) increase the supervision activities of the EDPS (inspections, compliance visits, guidelines) and (ii) better reflect the weight given to supervision in the Regulation (subject to our comment above). ▶ A secretariat has been created. The EDPS Rules of Procedure specify the rules governing the appointment and tasks of the EDPS Secretariat.
Article 44 Independence	1. The European Data Protection Supervisor shall act in complete independence in the performance of his or her duties. 2. The European Data Protection Supervisor shall, in the performance of his or her duties, neither seek nor take instructions from anybody. 3. The European Data Protection Supervisor shall refrain from any action incompatible with his or her duties and shall not, during his or her term of office, engage in any other occupation, whether gainful or not. 4. The European Data Protection Supervisor shall, after his or her term of office, behave with integrity and discretion as regards the acceptance of appointments and benefits.	**Case law** ▶ The establishment of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of personal data (see notably, Case 288-12, paragraph 48, Case C-518/07 Commission v Germany EU:C:2010:125, paragraph 23, and Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37)[44]. ▶ In Commission v Germany (Case C-518/07, paragraph 30)[45], the Court ruled on the meaning of the expression "with complete independence" by stating that a supervisory authority must be free from any direct or indirect external influence. **Implementation and application** ▶ The Supervisory authority must carry out its activities in total independence. This independence includes the obligation to

[44] CJEU, 8 April 2014, European Commission v. Hungary, Case C-288/12 ; CJEU, 9 March 2010, European Commission v. Federal Republic of Germany, Case C-518/07: CJEU, 16 October 2012, European Commission v Republic of Austria, Case C-614/10.
[45] CJEU, 9 March 2010, European Commission v Federal Republic of Germany, Case C-518/07.

ARTICLE BY ARTICLE ANALYSIS		
		allow the Supervisor to exercise his duties without any external influence and to serve his or her full term of office (Case 288-12, paragraph 62). ▶ The operational independence to carry out the tasks is not sufficient to protect against any external influence (Case 288-12, paragraph 52)[46]. ▶ In addition to the criteria of independence required during the appointment procedure (see above), the independence of the EDPS and his or her Assistant is ensured by the implementing acts (e.g. the EDPS has its own budget and the Supervisors' salary, allowances and benefits are paid by the budget of the EDPS directly as per Decision 1247/2002/EC). The Rules of Procedures of the EDPS established in 2012 the principle of independence for the advisor (Article 3). Moreover, Article 15 of the EDPS Rules of Procedure also stipulates that the EDPS is an independent expert in the field of data protection bound by the principles of impartiality, integrity, transparency and pragmatism. Moreover, the EDPS is assisted by an autonomous secretariat.
Article 45 Professional secrecy	The European Data Protection Supervisor and his or her staff shall, both during and after their term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.	**Implementation and application** ▶ The EDPS has adopted an internal procedure for professional secrecy (recalled in several procedures and instruments). ▶ *See al*so Article 17 of the Staff Regulations and the confidentiality declarations signed by staff members when they join the EDPS. ▶ The EDPS staff is subject to strict confidentiality obligations and the duty of professional secrecy is appropriately applied

[46] CJEU, 8 April 2014, European Commission v Hungary, Case C-288/12.

ARTICLE BY ARTICLE ANALYSIS		
		by the EDPS, but this duty has raised some issues: • During the performance of inspections, some EU institutions and bodies require the inspectors to have security clearance. Security clearance is not mandatory to perform the EDPS tasks, except to access classified information. However, the EDPS is flexible and tries to select staff members who have security clearances in order to perform these audits. • In the course of legislative consultation institutions can be reluctant to submit to the EDPS legislative proposals impacting data protection or privacy that include highly confidential information. **Recommendation** ▶ Several tools and internal procedures allow for a satisfactory level of implementation and application of professional secrecy. However, increased communication on duty of secrecy of EDPS staff towards EU institutions and bodies could facilitate the performance of its duties.
Article 46 Duties	The European Data Protection Supervisor shall:	
	(a) hear and investigate complaints, and inform the data subject of the outcome within a reasonable period; (b) conduct inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;	**Implementation and application (see also Articles 32 and 33)** ▶ The EDPS has established internal and external procedures to handle complaints (*see* the Rules of Procedure, the complaints case manual, the position paper on "Monitoring and Ensuring Compliance with Regulation (EC) No 45/2001, 13 December 2010" and the online form on the EDPS website). The procedures are efficient, regularly updated, and meet day-to-

ARTICLE BY ARTICLE ANALYSIS		
		day operational needs. ▶ EDPS effectively hears and investigates complaints lodged by individuals (Article 32) or EU staff (Article 33). The EDPS may also decide to launch inquiries following a complaint. ▶ The number of complaints gradually increased until 2009. ▶ In some cases, the complaint results in an amicable solution without the need to adopt a formal decision. If an amicable settlement could not be reached, the EDPS adopts a formal decision. The EDPS has never sued an institution or body as a result of a complaint because, according to the EDPS, the EU institution or body has always complied with the final decision adopted by the EDPS. Sometimes, the case may escalate to the upper management and meetings may be organized. ▶ Any interested party can ask for a review by the EDPS of its decision (of 32 requests for review, only one had sufficient grounds according to the EDPS). ▶ The EDPS has established several filters to reduce the number of complaints that do not require an inquiry or an in-depth examination by the EDPS (notably, the EDPS has drawn up a standard complaint form that has proven to be effective). ▶ The complaint should first be submitted to the DPO of the EU institution or body concerned before lodging the complaint with the EDPS.
	(c) 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;**	**Implementation and application** ▶ The notion of "judicial capacity" has given rise to differing interpretations between the Court of Justice of the European Union and the EDPS regarding the publication of the names of the parties in a case brought before the Court of Justice. The Court of Justice has a more narrow definition of this notion. ▶ In addition to all the supervisory tools provided for by the

ARTICLE BY ARTICLE ANALYSIS		
		Regulation, the EDPS also monitors and supervises the application of Regulation (EC) No 45/2001 by conducting (i) biannual general surveys and (ii) compliance visits.
	(d) advise all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data;	*See also* 28.2 **Implementation and application (together with Article 28)** ▶ Pursuant to Article 28.2 of Regulation (EC) No 45/2001, one of the main tasks of the EDPS is to examine the data protection and privacy impact of proposed new legislation. Regulation (EC) No 45/2001 does not detail the consultation procedure but states that the European Commission "*when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, shall consult the European Data Protection Supervisor*". ▶ The EDPS also advises EU institutions and bodies on the basis of the consultation received. DPOs and data controllers have indicated that the responses to consultation are not always suitable for day-to-day practices and not always provided in a timely manner. ▶ The EDPS has also set up a hotline in order to advise EU institutions and bodies.
	(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;	**Implementation and application** ▶ The EDPS has implemented this obligation in Article 38 of the EDPS Rules of Procedure. ▶ The EDPS effectively applies this obligation: o Collects and uses publicly available information about new technology developments and meets with

ARTICLE BY ARTICLE ANALYSIS		
		industry constructors, experts and technology professionals. ○ Checks the claims and risks raised by the technology community regarding a specific technology and personal data protection. ▶ At the end of this process, the EDPS delivers its recommendations and guidelines in the technical area (i.e. future guidelines regarding data protection for mobile technologies, cloud computing and websites).
	(f) (i) cooperate with the national supervisory authorities referred to in Article 28 of Directive 95/46/EC in the countries to which that Directive applies to the extent necessary for the performance of their respective duties, in particular by exchanging all useful information, requesting such authority or body to exercise its powers or responding to a request from such authority or body; (ii) also cooperate with the supervisory data protection bodies established under Title VI of the Treaty on European Union particularly with a view to improving consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance; (g) participate in the activities of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up by Article 29 of Directive 95/46/EC;	**Implementation and application** ▶ The cooperation tasks of the EDPS are aimed at increasing the consistency of data protection in the EU. The implementation of cooperation efforts is laid down in Article 46 of the EDPS Rules of Procedure: ○ *"The EDPS shall take part with national supervisory authorities in the coordinated supervision of large scale IT systems, as provided under Union law.* ○ *The EDPS shall organize coordination meetings and provide the secretariat of the coordination groups.* ○ *The EDPS shall cooperate with individual national supervisory authorities to the extent necessary and according to their priorities, with a view to ensuring coordinated supervision of the national and central parts of large scale IT systems."* ▶ The EDPS cooperates with national data protection authorities mainly via the Article 29 Working Party. ▶ The EDPS' direct cooperation with national authorities is an area of increasing importance in the context of the

ARTICLE BY ARTICLE ANALYSIS		
		development of large-scale international databases such as EURODAC, the Visa Information System (VIS), the Schengen Information System II (SIS II) or the Customs Information System (CIS), which requires a coordinated approach to supervision.[47] Special legislation is applicable to these activities. The EDPS provides the secretariat for those Coordinated Supervision groups and was the chair of some of these Coordinated Supervision Groups for the EURODAC, VIS and CIS SCGs, for example. The EDPS also organizes meetings. The supervision groups monitor the systems (compliance with special legislation and functionalities provided for by Regulation (EC) No 45/2001) and draft recommendations (ensuring the existence of appropriate security and confidentiality measures). ▶ Even if this is not specifically provided for by Regulation (EC) No 45/2001, the EDPS also **participates in European and international conferences such as the Conference of Data Protection and Privacy Commissioners and in International Association of Privacy Professionals (IAPP) conferences**. ▶ The EDPS attends meetings of the Consultative Committee of Convention 108. In addition, the EDPS contributes to several panels and workshops on data protection in international organizations. On an international level, the EDPS also collaborates with data protection authorities of non-EU countries. This exchange of information at an international level ensures **consistency in the field of data protection, mutual assistance for the protection of personal data and engagement in data protection activities.** Cooperation on enforcement of data protection rules also occurs.

[47] 2013 EDPS Annual report.

ARTICLE BY ARTICLE ANALYSIS		
		▶ There is limited cooperation between the EDPS and the Joint Supervisory Bodies. **Recommendations** ▶ Regulation (EC) No 45/2001 does not foresee the role of the EDPS regarding international cooperation. In this respect, an amendment of Regulation (EC) No 45/2001 would bring the legislation in line with the current practices of the EDPS.
	(h) determine, give reasons for and make public the exemptions, safeguards, authorisations and conditions mentioned in Article 10(2)(b),(4), (5) and (6), in Article 12(2), in Article 19 and in Article 37(2);	**Implementation and application** ▶ The EDPS is drawing up opinions.
a	(i) keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the Data Protection Officers under Article 26;	**Implementation and application** ▶ The EDPS keeps a register of prior checking processes notified.
	(j) carry out a prior check of processing notified to him or her;	**Implementation and application** ▶ Pursuant to Articles 27 and 46 of Regulation (EC) No 45/2001, the EDPS carries out a prior check of notification received. These provisions of Regulation (EC) No 45/2001 are effectively implemented by the EDPS Rules of Procedure, which complete and interpret the prior check procedure laid down by Regulation (EC) No 45/2001 (Articles 19 to 23). Position paper on "Monitoring and Ensuring Compliance with Regulation (EC) No 45/2001, 13 December 2010" also completes the applicable rules and procedures. Moreover, 74

ARTICLE BY ARTICLE ANALYSIS		
		▶ % of EU institutions and bodies consulted indicate that procedures relating to the notification of processing operations subject to prior check have been adopted. ▶ The EDPS efficiently performs prior checking. ▶ See also Article 27
	(k) establish his or her Rules of Procedure.	▶ Under Article 46 (k), the EDPS adopted its Rules of Procedure in December 2012.[48] These rules take stock of the substantial experience of the EDPS in the field of data protection. This document adds to and interprets the rules and principles laid down in Regulation (EC) No 45/2001. Some procedures as the rules governing the cooperation and the cooperation with Data Protection Officers were not foreseen by Regulation (EC) No 45/2001. ▶ The Rules of Procedure lay down the core values and rules governing the general administration of the independent authority (Chapter I- Chapter IV). They also set forth detailed rules with regard to the procedures and rules applied in the performance of the supervisory and consultation tasks (Chapter V. Specific Procedure).
Article 47 Powers	1. The European Data Protection Supervisor may: (a) give advice to data subjects in the exercise of their rights; (b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;	▶ Case C-73/07 (12 September 2007)[49]: Order of the President pursuant to which the EDPS cannot intervene in preliminary ruling proceedings **Implementation and application** ▶ The EDPS' powers are thoroughly implemented in the EDPS Rules of Procedure and various other position papers.

[48] Decision of the European Data Protection Supervisor of 17 December 2012 on the adoption of Rules of Procedure.

[49] CJEC, Order of the President of the Court, 12 September 2007, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy,Case C-73/07.

ARTICLE BY ARTICLE ANALYSIS		
	(c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19; (d) warn or admonish the controller; (e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed; (f) impose a temporary or definitive ban on processing; (g) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission; (h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty; (i) intervene in actions brought before the Court of Justice of the European Communities.	▶ The EDPS' range of powers is extensive. ▶ First, the EDPS will refer the matter to the data controller (Article 47 (b)) and will check whether the request has been first provided to the DPO. Article 47 (c) and (e) are the most commonly used powers. Moreover, the EDPS has intervened in several cases before the Court of Justice (*see below*). ▶ The EDPS does not apply its sanctioning powers even though the appropriateness of the powers is not questioned by the stakeholders. The EDPS has rarely used its power to warn or admonish the data controller. The EDPS has only banned processing operations in limited cases. Article 47 (g) and Article 47 (h) have never been used either. ▶ The powers are not used but are very efficient, according to the EDPS. The perception of DPOs varies substantially insofar as several DPOs consider that the inefficiency of the sanctions results in a low level of enforcement of the Regulation provisions by the management (*see also* Article 49). **Recommendation** ▶ The enforcement of Regulation provisions relating to sanctions must be enhanced.
	(i) intervene in actions brought before the Court of Justice of the European Communities.	**Implementation and application** ▶ This power is implemented by the EDPS Rules of Procedure (Article 41). An internal manual has also been established and is used by the EDPS. The pleadings submitted at oral hearings (where applicable) are published on the EDPS website. ▶ This power to intervene before the Court of Justice in

ARTICLE BY ARTICLE ANALYSIS		
		accordance with Article 40 of the Statute of the Court of Justice of the European Union[50] is effectively applied by the EDPS, but limited, as EDPS may solely intervene in proceedings designed to resolve a dispute in support of one party. This means that the EDPS has to choose which party to support, despite lacking access to the materials of the case, i.e. sufficient information. The Court held that the right to intervene does not extend to preliminary reference procedures under Article 267 TFEU (see order of the President in Case C-73/07)[51]. The EDPS highlighted the necessity of being recognized as *amicus curiae* before the Court of Justice (and not only in support of one party) and of being provided with the possibility to submit observations during the preliminary reference proceedings. It should be stressed that the Court of Justice has already invited the EDPS to attend hearings in the course of preliminary ruling proceedings (pursuant to Article 24 of the Statute).[52] Once the leave for intervention has been granted by the Court of Justice of the European Union, the channels for

[50] OJ C 83/210.

[51] According to the Order of the President of the Court in case C-73/07 §11 & 12.

" *11 Participation in the proceedings in the cases covered by Article 234 EC is governed by Article 23 of the Statute of the Court of Justice, which limits the right to submit statements of case or observations to the Court to the parties, the Member States, the Commission of the European Communities and, where appropriate, the Council of the European Union, the European Parliament and the European Central Bank, to the States, other than the Member States, which are parties to the Agreement on the European Economic Area, the EFTA Surveillance Authority and non-member States. By the expression 'parties', Article 23 refers only to the parties to the action before the national court (see, to that effect, the judgment in Bollmann, paragraph 4, and the order of the President of the Court in SGAE, paragraph 5).*

12 Since the Supervisor is not expressly mentioned in Article 23 of the Statute of the Court of Justice, and since, in the main proceedings, he is not a 'party' for the purposes of that Article, he is not entitled to submit observations to the Court on the questions referred by the national court for a preliminary ruling."

[52] CJEC, Order of the President of the Court, 12 September 2007, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy,Case C-73/07.

.

ARTICLE BY ARTICLE ANALYSIS		
		communication are smooth thanks to the use of e-curia. **Recommendation** ▶ The EDPS power of intervention before the Court is implemented and applied. Some practical drawbacks have been pointed out by the EDPS. The evaluator, however, with due regard to the independence of the Court of Justice of the European Union, does not recommend tackling practical drawbacks by amending Regulation (EC) No 45/2001.
	2. The European Data Protection Supervisor shall have the power: (a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries; (b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there. **Recital** (23) The independent supervisory authority should exercise its supervisory functions in accordance with the Treaty and in compliance with human rights and fundamental freedoms. It should conduct its enquiries in compliance with the Protocol on Privileges and Immunities and with the Staff Regulations of Officials of the European Communities and the conditions of employment applicable to Other Servants of the Communities.	**Implementation and application (together with Article 46(b))** ▶ The procedure on inspection is implemented in an internal manual. Inspections are part of an Annual Inspection Planning. ▶ According to the EDPS, the institutions/bodies to be investigated are chosen on the basis of objective criteria (social factors, suspicion arising from a complaint, transfer to non-EU country, etc.). ▶ After the "on-the-spot" activities, the EDPS provides the institution inspected with a final report including feedback. The EDPS follows up the inspections and monitors the implementation of the recommendations drawn up in the inspection report. ▶ In order to effectively raise awareness of institutions and increase collaboration with institutions and bodies, the EDPS has devoted more time to inspections. Efficiency has increased over time thanks to the adoption of revised workflows and procedures (in particular, the internal manual). ▶ The relationships between the EDPS and DPOs during inspections are constructive and allow for increased effectiveness.

ARTICLE BY ARTICLE ANALYSIS		
		▶ Nevertheless, major criticisms have been raised by DPOs: o the inspections are remote from the operational activities of the EU institution or body at stake (i.e. the EDPS does not have the appropriate work-field experience); o the follow-up is not performed in a timely manner (sometimes two years after the inspections); o the number of inspections is too limited; o the inspections are more like audits than real inspections.
Article 48 Activities report	1. The European Data Protection Supervisor shall submit an annual report on his or her activities to the European Parliament, the Council and the Commission and at the same time make it public. 2. The European Data Protection Supervisor shall forward the activities report to the other Community institutions and bodies, which may submit comments with a view to possible examination of the report in the European Parliament, in particular in relation to the description of the measures taken in response to the remarks made by the European Data Protection Supervisor under Article 31. **Recital** (25) The decisions of the independent supervisory authority regarding exemptions, guarantees, authorisations and conditions relating to data processing operations, as defined in this Regulation, should be published in the activities report. Independently of the publication of an annual activities report, the independent supervisory authority may publish reports on specific subjects.	**Implementation and application** ▶ The first annual report was published on 18 March 2005 and took stock of the first year of existence of the EDPS (from 17 January 2004 to 31 December 2004). Each year, an annual report has been submitted to the European Parliament, the Commission and the Council and published, together with an executive summary and a press release (only available from 2004-2007). All the reports are available on the EDPS website at least in English and French. The reports provide a comprehensive overview of the activities of the EDPS. Specific "Activities reports" are also published on the EDPS website. ▶ It appears that the report is not forwarded to EU institutions and bodies for comments. However, the EDPS is keen to receive feedback and comments from DPOs, DPCs and data controllers. ▶ Other reports are also published by the EDPS such as reports on strategy.[53]

[53] https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Strategy2015.

ARTICLE BY ARTICLE ANALYSIS		
Chapter VI FINAL PROVISIONS		
Article 49 Sanctions	Any failure to comply with the obligations pursuant to this Regulation, whether intentionally or through negligence on his or her part, shall make an official or other servant of the European Communities liable to disciplinary action, in accordance with the rules and procedures laid down in the Staff Regulations of Officials of the European Communities or in the conditions of employment applicable to other servants.	**Implementation and application** ▶ The evaluator is not aware of any implementing rules on sanctions. ▶ Offenders are never (or extremely rarely) sanctioned for failures to comply with the rules enshrined in the Regulation. Disciplinary proceedings are almost never initiated against an offender on the basis of the Staff Regulations or the conditions of employment applicable to other servants. ▶ As a result, this reduces controllers' incentive to comply with the Regulation provisions and substantially hinders the enforcement of the Regulation. **Recommendation** ▶ The enforcement of the Regulation provisions relating to sanctions must be enhanced.
Article 50 Transitional period	Community institutions and bodies shall ensure that processing operations already under way on the date this Regulation enters into force are brought into conformity with this Regulation within one year of that date.	▶ No particular comment is called for.
Article 51 Entry into force	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Communities. This Regulation shall be binding in its entirety and directly applicable in all Member States.	▶ No particular comment is called for.
ANNEX		

ARTICLE BY ARTICLE ANALYSIS		
ANNEX 1.	The Data Protection Officer may make recommendations for the practical improvement of data protection to the Community institution or body which appointed him or her and advise it and the controller concerned on matters concerning the application of data protection provisions. Furthermore he or she may, on his or her own initiative or at the request of the Community institution or body which appointed him or her, the controller, the Staff Committee concerned or any individual, **investigate matters and occurrences directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller.** 2. The Data Protection Officer may be consulted by the Community institution or body which appointed him or her, by the controller concerned, by the Staff Committee concerned and by any individual, without going through the official channels, on any matter concerning the interpretation or application of this Regulation. 3. No one shall suffer prejudice on account of a matter brought to the attention of the competent Data Protection Officer alleging that a breach of the provisions of this Regulation has taken place. 4. Every controller concerned shall be required to assist the Data Protection Officer in performing his or her duties and to give information in reply to questions. In performing his or her duties, the Data Protection Officer shall have access at all times to the data forming the subject-matter of processing operations and to all offices, data-processing installations and data carriers. 5. To the extent required, the Data Protection Officer shall be relieved of other activities. The Data Protection Officer and his or her staff, to whom Article 287 of the Treaty shall apply, shall be required not to divulge information or documents which they obtain in the course of their duties.	▶ Description of the tasks of the DPO : *see* Article 24

ARTICLE BY ARTICLE ANALYSIS		
RECITALS		
Consistency	*(12) Consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data should be ensured throughout the Community.*	▶ Recital 12 (together with Recital 32, Article 24.1(c) and 46(c)) ▶ Over time, coherence and consistency tools have been implemented by EU institutions and bodies. These tools are efficient tools to ensure the consistency and coherence of the application of the rules and principles. ▶ The EDPS has developed tools (guidance, training) in order to ensure that the DPOs have access to the same level of information on data protection matters. ▶ The DPOs have developed the DPO network. ▶ Networks of Data Protection Coordinators (DPC) have also been established in certain EU institutions and bodies.
Particulars of the EU institutions and bodies	*(20) The provisions applicable to the Community institutions and bodies should correspond to those provisions laid down in connection with the harmonisation of national laws or the implementation of other Community policies, notably in the mutual assistance sphere. It may be necessary, however, to specify and add to those provisions when it comes to ensuring protection in the case of the processing of personal data by the Community institutions and bodies.* *(21) This holds true for the rights of the individuals whose data are being processed, for the obligations of the Community institutions and bodies doing the processing, and for the powers to be vested in the independent supervisory authority responsible for ensuring that this Regulation is properly applied.*	▶ The rules applicable to EU institutions and bodies should be brought into line with those applicable to Member States. However, the specificities of the EU institutional framework should be taken into consideration.