SUMMARIES OF EU COURT DECISIONS RELATING TO DATA PROTECTION 2000-2015

PREPARED BY LARAINE LAUDATI
OLAF DATA PROTECTION OFFICER

28 JANUARY 2016
10TH EUROPEAN DATA PROTECTION DAY

DATA PROTECTION OFFICER

EUROPEAN ANTI-FRAUD OFFICE

Introduction

In honour of the celebration of the Tenth European Data Protection Day on 28 January 2016, I have prepared this document in order to help OLAF management, investigators, and other staff to have easy access to the judgments of the European Union courts concerning data protection. The judgments span a period of more than 15 years, from the first decisions in 2000 through the landmark decisions taken in 2015.

The summaries are organised both by case (in chronological order of case number) and by topic. The case summaries present a brief description of facts and issues before the court in each case, as well as a summary of the holdings of the court together with the reference paragraph numbers from the court's judgment. The topical summaries list the holdings from each case relating to the listed topic.

This document is designed to be a reference tool to facilitate the work of finding relevant caselaw. However, it should not be relied upon on its own; the court judgment itself must always be consulted directly.

As OLAF's Data Protection Officer for the past ten years, I have had the opportunity to experience the implementation of data protection in an EU body first hand, from the first days when we struggled to develop the necessary tools, to the present when data protection at OLAF is accepted as part of our daily business. I have watched the caselaw develop over these years, and worked to determine what implications each decision might have for the implementation of data protection at OLAF. I would like to share this tool for ready reference to the caselaw, which I have updated each year for my own use. I hope that it will be useful to my colleagues at OLAF and more broadly to other data protection professionals.

Laraine Laudati
OLAF Data Protection Officer

Table of Contents

I. SUMMARY OF EU COURT DECISIONS RELATING TO DATA PROTECTION (IN NUMERICAL ORDER OF CASE NUMBER)

1. COURT OF JUSTICE DECISIONS

1.1. C-450/00, COMMISSION V. LUXEMBOURG, 4.10.2001 ("LUXEMBOURG")

Infringement procedure against Luxembourg for failure to bring into force, within the prescribed period, the laws, regulations and administrative provisions necessary to comply with Directive 95/46/EC, as required under Article 32 of the Directive.

Transposition: Luxembourg argued that its delay in transposing the Directive was due to the new distribution of ministerial powers following a change in its internal government. The Court ruled that a Member State may not plead provisions, practices or circumstances in its internal legal system in order to justify a failure to comply with obligations and time limits laid down in a Directive, and thus a violation had occurred. (¶¶ 8-9)

1.2. C-465/00 AND C-138/01, RECHNUNGSHOF V. OSTERREICHISCHER RUNDFUNK, 20.5.2003 ("RECHNUNGSHOF")

Reference for a preliminary ruling by the Austrian Constitutional and Supreme courts. National legislation required public bodies subject to the control of the Rechnungshof (Court of Audit) to communicate to it the salaries and pensions exceeding a certain level paid by them to their employees and pensioners, together with the names of the recipients, for the purpose of it drawing up an annual report to be transmitted to the federal and provincial legislatures, and the general public. The defendants, subject to this requirement, refused, claiming that they are not obliged to communicate such data relating to income on grounds of data protection requirements.

Questions referred: (1) Whether data protection law precludes national legislation which requires a state body to collect and transmit data on income for the purpose of publishing the names and income of various state employees; (2) Whether provisions precluding such national legislation are directly applicable, in the sense that the persons obliged to disclose may rely on them to prevent the application of the national provisions.

Scope of Directive 95/46: Applicability of Directive 95/46 cannot depend on whether the specific situations at issue have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty (here free movement of workers). The EU system of data protection has a wide scope, is defined in very broad terms, and does not depend on whether, in every specific case, the processing of personal data has a connection to the free movement between the Member States. A contrary interpretation could make the limits of the field of application of the Directive unsure and uncertain. The system consists of checks and balances in which processing of personal data is subject to a number of conditions and limitations. (¶¶ 42-43)

Article 8 ECHR: Provisions of Directive 95/46, insofar as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must be interpreted in light of that right, which forms an integral part of the general principles of EU law. Article 8 ECHR states that public authorities must not interfere with the right to respect for private life, unless it is in accordance with law and is necessary in a democratic society to protect certain interests. (¶¶ 70-71)

The collection of data by name relating to an individual's professional income, with a view to communicating it to third parties, falls within the scope of Article 8. The ECtHR has held that communication of the data infringes the right of the persons concerned to respect for private life. (¶¶ 73-74)

Regarding necessity, the purpose of the provision was to keep salaries within reasonable limits, which fits within the "economic well-being of the country". But "necessary" means that a pressing social need is involved and the measure is proportionate to the legitimate aim pursued. The

authorities enjoy a margin of appreciation. The interests of the state must be balanced against the seriousness of the interference. The interference is justified only insofar as publication of the names is both necessary and appropriate to the aim of keeping salaries within reasonable limits, which is for the national court to examine. If not, then the interference also constitutes a violation of Articles 6 and 7 of Directive 95/46. (¶¶ 82-90, 94)

Direct applicability: Wherever provisions of a directive appear to be unconditional and sufficiently precise, they may, in the absence of implementing measures adopted within the prescribed period, be relied on against any incompatible national provision, or insofar as they define rights which individuals are able to assert against the State. (¶ 98)

1.3. C-101/01, LINDQUIST, 6.11.2003 ("LINDQUIST")

Reference for a preliminary ruling by the Swedish appellate court. Mrs. Lindquist had published on the internet the names, jobs, hobbies, telephone numbers, family circumstances etc. of 18 colleagues, as well as the fact that one had injured her foot and was on medical leave. She removed the data as soon as some objected. She was charged with criminal violations of Swedish data protection law.

Questions referred: (1) Whether the mention of a person, by name or with name and telephone number, on an internet home page is an action which falls within the scope of Directive 95/46; (2) If so, whether the loading of information of this type about work colleagues onto a private home page which is accessible to anyone who knows its address is covered by one of the exceptions under Article 3(2) of Directive 95/46; (3) Whether information on a home page stating that a named colleague has injured her foot and is on half-time on medical grounds is personal data concerning health which, according to Article 8(1), may not be processed; (4) Whether the loading of the data onto the home page, with the result that the data becomes accessible to people in third countries, constitutes a transfer to a third country; (5) Whether a Member State can provide more extensive protection for personal data than the directive.

Definition of personal data: The name of a person in conjunction with his/her telephone number, and information about working conditions or hobbies constitute personal data. (¶ 24)

Definition of processing: The operation of loading personal data on an internet page must be considered to be processing. (¶ 25)

Scope of Directive 95/46: Loading personal data on an internet page is processing by automatic means. (¶ 25)

Processing for purely personal or household activity: Mrs. Lindquist's activities were mainly charitable and religious, but these are not covered by the exceptions in Article 3(2) of the Directive and cannot be considered exclusively personal or domestic. (¶¶ 45-47)

Sensitive personal data: Reference to the fact that an individual has injured her foot and is on medical leave constitutes personal data concerning health within the meaning of Article 8(1), as that provision must be given a wide interpretation so as to include all aspects, both physical and mental, of the health of an individual. (¶¶ 50-51)

Transfers to third countries: The publication on the internet did not constitute a transfer, as an internet user would have to connect to the internet and personally carry out the necessary actions to consult those pages. Mrs. Lindquist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access. There is no transfer of data to a third country within the meaning of Article 25 of the Directive when an individual in a Member State loads personal data onto an internet page which is stored with his/her hosting provider in that or another Member State, thereby making the data accessible to anyone who connects to the internet, including people in a third country. (¶¶ 60-61, 68, 70)

Balancing fundamental rights: The data protection and freedom of expression must be balanced against each other, and the regime of the Directive provides in itself multiple mechanisms allowing a balancing of the different fundamental rights to be carried out. Therefore, it is not a disproportionate violation of the principle of freedom of expression. (¶¶ 82-87, 90)

Transposition/Harmonisation: The Directive envisages complete harmonisation, thus Member States must adopt national legislation conforming to the regime of the Directive. However, certain provisions of the Directive can explicitly authorize the Member States to adopt more constraining regimes of protection. This must be done in accordance with the objective of maintaining a balance between free movement of personal data and protection of private life. In addition, Member States remain free to regulate areas excluded from the scope of application of the Directive in their own way, provided no other provision of EU law precludes it. (¶¶ 96-99)

1.4. C-317 AND 318/04, PARLIAMENT V. COUNCIL (PNR), 30.5.2006 ("PNR")

Action for annulment by the European Parliament of Council Decision 2004/496/EC concerning the conclusion of an agreement between the EU and the USA on the processing and transfer of Passenger Name Record (PNR) data and on the adequacy decision on data transferred to the USA, both of which were adopted on the basis of Directive 95/46. After the 11 September 2011 terrorist attacks, the US passed legislation providing that air carriers operating flights to or from the US or across the US had to provide US customs with electronic access to the data contained in their automated reservation and departure control systems (PNR). Negotiations followed, and in April 2004, the Commission adopted the decision on adequacy and the Council adopted the decision on conclusion of an agreement between the EU and the US on the processing and transfer of PNR data.

Appropriate legal basis:

- Adequacy decision: Requirements for transfer were based on a statute enacted by the USA in November 2001 and implementing Regulations adopted thereunder, which concern enhancement of security and conditions under which persons may enter and leave the USA, fighting against terrorism and fighting transnational crime. Thus, the transfer of PNR data is processing concerning public security. (¶¶ 55-56)

  Even though PNR data are initially collected in the course of commercial activity, the processing addressed in the adequacy decision concerns safeguarding public security and law enforcement. The facts that the data are collected by private operators for commercial purposes and that those operators arrange for the transfer of the data to the third country does not prevent that transfer from being regarded as processing excluded from the Directive's scope. Thus, it falls within the first indent of Article 3(2) of the Directive, which excludes from the Directive's scope data protection in the course of activities provided for by Titles V and VI of the EU Treaty. Accordingly, the adequacy decision is annulled. (¶¶ 57-61)

- Agreement: Article 95 of the EC Treaty (internal market) in conjunction with Article 25 of the Directive (transfers to third countries ensuring adequacy) do not justify EU competence to conclude the Agreement. The agreement relates to the same transfers as the adequacy decision, and thus processing operations are outside the scope of the Directive. The Council decision approving the conclusion of the agreement between the EU and the US on the processing of PNR data is annulled. (¶¶ 67-70)

1.5. C-275/06, PROMUSICAE, 29.1.2008 ("PROMUSICAE")

Reference for a preliminary ruling by the Juzgado de lo Mercantil No. 5 de Madrid. Telefonica had refused to disclose to Promusicae, an NPO acting on behalf of its members who are holders of intellectual property rights, personal data relating to users of the internet who accessed the KaZaA file exchange program and shared files of recordings of Promusicae's members, by means of connections provided by Telefonica. Promusicae wanted to bring civil actions against those persons.

Question referred: Whether EU law permits Member States to limit the duty of operators of telecom networks to supply traffic data.

Balancing fundamental rights: The requirements of protection of different fundamental rights must be reconciled, namely the right to respect for private life on the one hand and rights to protection of property and an effective remedy on the other hand. Directive 2002/58 provides rules determining in what circumstances and to what extent personal data processing is lawful and what safeguards must be provided. (¶¶ 65-66)

Transposition/Harmonisation: Directives 2000/31, 2001/29, 2004/48 and 2002/58 do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in civil proceedings, nor does it oblige them to impose such an obligation. However, when transposing various intellectual property Directives, Member States must take care to interpret them such that there is a fair balance struck between the various fundamental rights protected by the Community legal order. Further, when implementing the national law transposing those Directives, authorities and courts of the Member States must interpret them in a manner consistent with the Directives and make sure that the interpretation does not conflict with those fundamental rights or other general principles of Community law, such as the proportionality principle. (¶ 70)

1.6. C-301/06, IRELAND V. PARLIAMENT AND COUNCIL, 10.2.2009 ("IRELAND")

Action for annulment by Ireland regarding Directive 2006/24/EC on the retention of electronic communication data on the ground that it was not adopted on an appropriate legal basis (Article 95 EC Treaty), amending Directive 2002/58 (also based on Article 95).

Appropriate legal basis: The Court rejected Ireland's argument that the sole or principal objective of the Directive is investigation, detection and prosecution of crime. Article 95(1) provides that the Council is to adopt measures for approximation of provisions laid down by law, regulation or administrative action in the Member States which have the objective of establishment and functioning of the internal market. It may be used where disparities exist (or are likely to exist in the future) between national rules which obstruct fundamental freedoms or create distortions of competition and thus have a direct effect on the functioning of the internal market. The premise of the Directive was to harmonize disparities between national provisions governing retention of data by service providers, particularly regarding the nature of data retained and periods of data retention. It was apparent that differences were liable to have a direct impact on the functioning of the internal market which would become more serious with the passage of time. (¶¶ 62-71)

Article 47 of the EU Treaty provides that none of the provisions of the EC Treaty may be affected by a provision of the EU Treaty, in order to safeguard the building of the *acquis communautaire*. Insofar as Directive 2006/24 comes within the scope of Community powers, it could not be based on a provision of the EU Treaty without infringing Article 47. Directive 2006/24 provisions are limited to activities of service providers and do not govern access to data or use thereof by police or judicial authorities of the Member States. They are designed to harmonize national laws on the obligation to retain data, the categories of data to be retained, the periods of retention of data, data protection and data security, and the conditions for data storage. They do not involve intervention by police or law enforcement authorities of Member States, nor access, use or exchange by them. Thus Directive 2006/24 relates predominantly to the functioning of the internal market. (¶¶ 75, 78, 80-83)

1.7. C-524/06, HUBER V. GERMANY, 16.12.2008 ("HUBER")

Reference for a preliminary ruling by the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Germany). Huber, an Austrian national resident in Germany, requested the deletion of personal data relating to him (name, date and place of birth, nationality, marital status, sex, entries and exits from Germany, residence status, particulars of passports, statements as to domicile, reference numbers) in the German Central Register of Foreign Nationals (AZR). The Bundesamt assists public authorities responsible for the application of the law related to foreign nationals and asylum. The AZR is used for statistical purposes and by security and police services and judicial authorities for the prosecution and investigation of criminal activities. Germany rejected Huber's request.

Question referred: Whether the processing of personal data of an Austrian national in the AZR is compatible with the requirement of necessity under Article 7(e) of Directive 95/46.

Scope of Directive 95/46: Article 3(2) excludes from the scope of Directive 95/46 the processing of personal data concerning public security, defense, and criminal law activities. Thus, in this case, only processing for a purpose relating to the right of residence and for statistical purposes falls within the scope of Directive 95/46. (¶¶ 44-45)

Necessity: In light of the fact that Directive 95/46 is intended to ensure an equivalent level of data protection in all Member States, to ensure a high level of protection in the EU, the concept of

necessity in Article 7(e) cannot have a meaning which varies among Member States. Thus, it is a concept which has its own independent meaning in EU law, and must be interpreted in a manner which fully reflects the objective of Directive 95/46. (¶¶ 50-52)

Under EU law, the right of free movement of a Member State national is not unconditional, but may be subject to limitations and conditions imposed by the Treaty and implementing rules. Legislation provides that a Member State may require certain documents to be provided to determine the conditions of entitlement to the right of residence. Thus, it is necessary for a Member State to have relevant particulars and documents available to it in order to ascertain whether a right of residence in its territory exists. Use of a register to support authorities responsible for application of the legislation on the right of residence is, in principle, legitimate. However, the register must not contain any information other than what is necessary for that purpose, and must be kept up to date. Only anonymous information is required for statistical purposes. Access must be restricted to the responsible authorities. The central register could be necessary if it contributes to a more effective application of that legislation. The national court should decide whether these conditions are satisfied. (¶¶ 54-62)

1.8. C-73/07, TIETOSUOJAVALTUUTETTU [FINNISH DATA PROTECTION OMBUDSMAN] V. SATAKUNNAN MARKKINAPORSSI OY AND SATAMEDIA OY, 16.12.2008 ("TIETOSUOJAVALTUUTETTU")

Reference for preliminary ruling by the Korkein hallinto-oikeus (administrative court, Helsinki). Defendant 1: (a) collected public personal data (the name of persons whose income exceeded a threshold, the amount of earned and unearned income, and the wealth tax levied) from Finnish tax authorities and (b) published extracts in a regional newspaper each year. The newspaper stated that personal data can be removed on request without charge. Defendant 1 also: (c) transferred the data on CD ROM to Defendant 2 (owned by the same shareholders) which (d) disseminated them by text messaging system.

Questions referred: (1) |Whether collection, publication, transfer of a CD ROM and text messages constitutes processing of personal data; (2) Whether it is processing for solely journalistic purposes within the meaning of Article 9 of Directive 95/46; (3) Whether Article 17 and principles of Directive 95/46 preclude publication of data collected for journalistic purposes and their onward transfer for commercial purposes; (4) Whether personal data that have already been published in the media fall outside scope of Directive 95/46.

Definition of personal data: Surname, given name of certain natural persons whose income exceeds certain thresholds as well as the amount of their earned and unearned income constitute personal data. (¶ 35)

Definition of processing: All four types of activities constitute processing of personal data. This includes personal data that have already been published in unaltered form in the media. Operations referred to in Article 2(b) must be classified as processing where they exclusively concern material that has already been published in unaltered form in the media. A general derogation from the application of the Directive in such a case would largely deprive the Directive of its effect. (¶¶ 35-37)

Scope of Directive 95/46: Only two exceptions to scope exist, which are set forth in Article 3(2). The first indent states that security and criminal law are activities of the state. The second indent states that processing by a natural person in the course of a purely personal or household activity concerns activities in the course of private or family life of individuals. Activities (c) and (d) are activities of private companies, and are not within the scope of Article 3(2). A general derogation from application of the Directive in respect of published information would largely deprive the Directive of its effect. Thus activities (a) and (b) are also not within the scope of Article 3(2). (¶¶ 39-49)

Processing for solely journalistic purposes: Article 1 of the Directive indicates that the objective is that Member States should, while permitting the free flow of personal data, protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy, with respect to processing of their personal data. That objective can only be pursued by reconciling those fundamental rights with the fundamental right to freedom of expression. The objective of Article 9 is to reconcile the two rights. Member States are required to provide derogations in relation to protection of personal data, solely for journalistic purposes or artistic or literary

expression, which fall within the fundamental right to freedom of expression, insofar as necessary for reconciliation of the two rights. To take account of the importance of the right of freedom of expression in every democratic society, it is necessary to interpret notions of freedom, such as journalism, broadly. Derogations must apply only insofar as strictly necessary. The fact that publication is done for profit making purposes does not preclude publication from being considered as "solely for journalistic purposes." The medium used is not determinative of whether it is "solely for journalistic purposes." Thus activities may be classified as "journalistic" if their sole object is the disclosure to the public of information, opinions or ideas, irrespective of the medium used to transmit them. (¶¶ 52-56, 59, 61)

1.9. C-518/07, COMMISSION V. GERMANY, 9.3.2010 ("GERMANY")

Infringement procedure against Germany, which transposed the second paragraph of Article 28(1) of Directive 95/46 (the requirement for an independent data protection Authority (DPA)) by making the authorities responsible for monitoring personal data processing outside the public sector in the different Lander subject to State oversight.

Independence of DPA: Independence normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure. There is nothing to indicate that the requirement of independence concerns exclusively the relationship between the supervisory authorities and the bodies subject to that supervision. The adjective "complete" implies a decision-making power independent of any direct or indirect external influence on the supervisory authority. The guarantee of independence of DPAs is intended to ensure the effectiveness and reliability of the supervision of compliance with data protection provisions, to strengthen the protection of individuals and bodies affected by their decisions. DPAs must act impartially and must remain free from any external influence, including that of the State or Lander. Independence precludes not only any influence exercised by supervised bodies, but also any directions or other external influence which could call into question the performance of those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data. (¶¶ 18-19, 25, 30)

State scrutiny in principle allows the government of the respective Land to influence the decision of the supervisory authority or cancel and replace those decisions. This is not consistent with the principle of independence.

1.10. C-553/07, COLLEGE VAN BURGEMEESTER EN WETHOUDERS VAN ROTTERDAM V. RIJKEBOER, 7.5.2009 ("RIJKEBOER")

Reference for a preliminary ruling by the Raad van State (Netherlands). Dutch law on personal data held by local authorities provides that on request, the Board of Aldermen must notify a data subject within four weeks whether his personal data have been disclosed to a purchaser or third party during the preceding year. Data held by the authority include basic data (name, date of birth, personal identification number, social security number, local authority of registration, etc.) and data on transfers. Mr. R requested to be informed of all instances where data relating to him were transferred in the preceding two years, and of the content and recipients. Dutch law on local authority personal records limited the communication of data to one year prior to the relevant request.

Questions referred: Whether the restriction provided for in the Netherlands law on local personal records on the communication of data to one year prior to the relevant request is compatible with Article 12(a) of Directive 95/46, whether read in conjunction with Article 6(1)(e) and the principle of proportionality.

Right of access: Right of access is necessary to enable the data subject to exercise his other rights (rectification, blocking, erasure, and notify recipients of same; object to processing or request damages). The right must of necessity relate to the past, otherwise the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for damages. Member States have some freedom of action in implementing the Directive, but it is not unlimited. Setting of a time limit on the right of access must allow the data subject to exercise his rights. It is for the Member States to fix a time limit for storage of information on the recipients and the content of the data disclosed, and to provide access to that information which constitutes a fair balance between the interest of the data subject in exercising his rights and the burden on the

controller to store that information. In the present case, limiting storage of information on recipients and content to one year, while the basic data is stored much longer, does not constitute a fair balance, unless it can be shown that longer storage would constitute an excessive burden. (¶¶51-57, 64-66)

1.11. C-557/07, LSG-GESELLSCHAFT ZUR WAHRNEHMUNG VON LEISTUNGSSCHUTZRECHTEN GMBH V. TELE2 TELECOMMUNICATION GMBH, 19.2.2009 ("LSG")

Reference for a preliminary ruling by the Oberster Gerichtshof (Austria). The applicant is a collecting society which, as trustee, enforces rights of recorded music producers in their worldwide recordings and of the recording artists in exploitation of those recordings in Austria. Tele2 is an Internet Service Provider (ISP) that assigns an IP address to its clients. LSG applied to the Austrian court for an order requiring Tele 2 to send names and addresses of persons to whom it had provided internet access service and whose IP addresses and date and time of connection were known.

Question referred (partial listing): Does Article 8(3) of Directive 2004/48, regard being had to Articles 6 and 15 of Directive 2002/58, not permit the disclosure of personal traffic data to private third parties for the purposes of civil proceedings for alleged infringements of exclusive rights protected by copyright?

Balancing fundamental rights: The judgment refers to ¶ 70 of the Promusicae judgment regarding balancing fundamental rights. That decision did not rule out the possibility that Member States may place an ISP under a duty of disclosure. An ISP provides a service which enables users to infringe copyright by providing a connection. (¶¶ 27, 43)

1.12. C-28/08, COMMISSION V. BAVARIAN LAGER CO., 29.6.2010 ("BAVARIAN LAGER")

Appeal by the Commission seeking annulment of the General Court judgment, which annulled the Commission's decision rejecting the request of the applicant (a trade association for German beer) for access to the full minutes of a meeting organized by the Commission (including names of attendees). The Commission had denied access to the names of five persons who attended the meeting, were members of a trade association and had not given consent to disclosure of their names, based on Article 4(1)(b) of Regulation 1049/2001. (The General Court decision which was the subject of appeal, as well as the Advocate General's opinion, are summarized below.)

Article 4(1)(b) exception: The General Court erred in limiting application of the exception in Article 4(1)(b) to situations in which privacy or the integrity of the individual would be infringed for the purposes of Article 8 of the ECHR and the caselaw of the European Court of Human Rights, without taking into account the legislation of the EU concerning the protection of personal data, particularly Regulation 45/2001. It disregarded the wording of the Article, which is an indivisible provision and requires that any undermining of privacy and the integrity of the individual must always be examined and assessed in conformity with the EU data protection legislation. The Article establishes a specific and reinforced system of protection of a person whose personal data could, in certain cases, be communicated to the public. (¶¶ 58-60)

Recital 15 of Regulation 45/2001 indicates legislative intent that Article 6 TEU and thereby Article 8 ECHR should apply where processing is carried out in the exercise of activities outside the scope of Regulation 45/2001 (Titles V and VI of pre-Lisbon TEU). Such reference was unnecessary for activities within the scope of Regulation 45/2001. Thus, where a request based on Regulation 1049/2001 seeks access to documents including personal data, Regulation 45/2001 becomes applicable in its entirety, including Articles 8 and 18. The General Court erred in dismissing the application of Article 8(b) and 18 of Regulation 45/2001, and its decision does not correspond to the equilibrium which the legislator intended to establish between the two Regulations. (¶¶ 62-65)

The Commission was right to verify whether the data subjects had given their consent to disclosure of personal data concerning them. By releasing the expurgated version of the minutes, with the names of five participants removed (three could not be contacted, two objected), the Commission did not infringe Regulation 1049/2001 and complied with its duty of openness. By requiring that regarding these five persons, the applicant establish the necessity for those personal data to be

transferred, the Commission complied with the provisions of Article 8(b) of Regulation 45/2001. As no necessity was provided, the Commission was not able to weigh up the various interests of the parties concerned, nor to verify whether there was any reason to assume that the data subjects' legitimate interests might be prejudiced, as required by Article 8(b). (¶¶ 75-78)

Definition of personal data: The General Court correctly held that surnames and forenames may be regarded as personal data. Thus, the list of names of participants in a meeting is personal data, since persons can be identified. (¶ 68)

Definition of processing: Communication of personal data in response to a request for access to documents constitutes processing. (¶69)

Opinion of Advocate General Sharpston, 15.10.2009

Scope of Regulation 45/2001: Article 3(2) should be construed to define the circumstances in which the Regulation applies ("the processing of personal data wholly or partly by automatic means and . . . 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.") Such processing of personal data by all Community institutions is then covered (applying Article 3(1)) insofar as it is "carried out in the exercise of activities all or part of which fall within the scope of Community law"). Other circumstances are not covered by Regulation 45/2001; they should be dealt with under Regulation 1049/2001, where requests are made to Community institutions for access to documents.

Article 4(1)(b) exception: Applicability of Regulation 1049/2001 versus Regulation 45/2001 in request for access to documents: B-1 documents contain an incidental mention of personal data, where the primary purpose of compiling the document has little to do with personal data. The raison d'être of such documents is to store information in which personal data are of minimal importance. B-2 documents contain a large quantity of personal data (e.g. a list of persons and their characteristics). The raison d'être of such documents is to gather together such personal data.

- Applications for B-1 documents should be handled under Regulation 1049/2001, while applications for B-2 documents should be handled under Regulation 45/2001, because they are within its scope by virtue of Article 3(2).

- Requests for B-1 documents do not require a reason, by virtue of Article 6(1) of Regulation 49/2001, while requests for B-2 documents will have to demonstrate the need for transfer of data, in accordance with Article 8(b) of Regulation 45/2001.

- Article 8 ECHR (including the justification test, where interference with privacy exists) must be applied with respect to an application for B-1 documents to determine whether personal data must be redacted, following Article 4(1)(b) of Regulation 45/2001. B-2 documents will be subject to the procedure outlined in Regulation 45/2001: processing must be lawful within the meaning of Article 5. The applicant will have to give reasons in accordance with Article 8; Article 9 applies for applications from non-Member States or non-Community international organizations; Article 10 applies regarding sensitive data; and Article 18 requires the institution to inform the data subject that he can object to processing.

- Disclosure under Regulation 1049/2001 of B-1 documents is *erga omnes*; disclosure under Regulation 45/2001 of B-2 documents is case-by-case and not *erga omnes*.

The first part of the exception applies to B-1 and B-2 documents; the second part applies only to B-2 documents.

General Court decision, T-194/04, 8.11.2007

Lawfulness: The right of access to documents of the institutions laid down by Article 2 of Regulation 1049/2001 constitutes a legal obligation for purposes of Article 5(b) of Regulation 45/2001. Therefore, if Regulation 1049/2001 requires communication of data, Article 5 of Regulation 45/2001 makes such communication lawful. (¶ 106)

Transfers: Access to documents containing personal data falls within the application of Regulation

1049/2001. Article 6(1) states that the applicant is not required to justify his request. Therefore, where personal data are transferred in the context of Regulation 1049/2001, the applicant does not need to prove necessity of disclosure of data for purposes of Article 8 of Regulation 45/2001, otherwise it would be contrary to the principle of the widest possible public access to documents held by the institutions. Exceptions must be interpreted narrowly. Given that access to a document will be refused under Article 4(1)(b) of Regulation 1049/2001 where disclosure would undermine protection of privacy and integrity of the individual, a transfer that does not fall under that exception cannot, in principle, prejudice the legitimate interests of the person concerned within the meaning of Article 8(b) of Regulation 45/2001. (¶¶ 107-108)

Right to object: The data subject has the right to object to processing, except in cases covered by Article 5(b), among others. Given that processing envisaged by Regulation 1049/2001 constitutes a legal obligation for purposes of Article 5(b), the data subject does not have a right to object. However, since Article 4(1)(b) of Regulation 1049/2001 lays down an exception to the obligation to provide access, it is necessary to consider the impact of disclosure on the data subject. If communication would not undermine protection of privacy etc., then the person's objection cannot prevent disclosure. (¶¶ 109-110)

Balancing fundamental rights: Regulation 45/2001 must be interpreted in light of fundamental rights which form an integral part of general principles of law with respect to which the ECJ ensures compliance. (¶ 111)

Article 8 ECHR: ECtHR caselaw interprets "private life" broadly, and there is no reason in principle to exclude professional or business activities from the concept of private life. To determine whether there is a breach of Article 8, it is necessary to determine (1) whether there has been an interference with private life of the data subject, (2) whether that interference is justified (i.e., it is in accordance with the law, pursues a legitimate aim, and is necessary in a democratic society – meaning that it is relevant and sufficient, and proportionate to the legitimate aims pursued). In cases concerning disclosure of personal data, the competent authorities have to be granted a certain discretion in order to establish a fair balance between competing public and private interests, subject to judicial review, referring to factors such as nature and importance of interests at stake and seriousness of interference. (¶114)

Any decision taken pursuant to Regulation 1049/2001 must comply with Article 8 ECHR. (¶ 116)

Article 4(1)(b) exception: To determine whether the exception applies, it is necessary to examine whether public access is capable of actually and specifically undermining the protection of the privacy and integrity of the persons concerned. (¶ 117)

The mere fact that a document contains personal data does not necessarily mean that privacy or integrity of the data subject is affected, even though professional activities are not, in principle, excluded from the concept of private life. Here, persons present at the meeting whose names were not disclosed were present as representatives of a trade association, and not in their personal capacity. Therefore, the fact that the minutes contain their names does not affect their private life. The minutes do not contain their personal opinions. Disclosure of the names is not capable of actually and specifically affecting the protection of privacy and the integrity of those persons. The mere presence of their name on the list does not constitute an interference. Regulation 45/2001 does not require the Commission to keep secret the names of persons who communicate opinions or information to it concerning the exercise of its functions. (¶¶ 123-126)

The court distinguishes the Osterreichischer Rundfunk decision on the ground that there, the specific combination of name and income received was at issue, in contrast to this case, where the name of persons acting in a professional capacity as representatives of a collective body is at issue, where no personal opinions can be identified. (¶ 127)

1.13. C-92/09 VOLKER UND MARKUS SCHECKE GBR V. LAND HESSEN, AND C-93/09, EIFERT V. LAND HESSEN AND BUNDESANSTALT FUR LANDWIRTSCHAFT UND ERNAHRUNG, 9.11.2010 ("SCHECKE")

Reference for a preliminary ruling by the Verwaltungsgericht Wiesbaden (Germany). A partnership established in the Land of Hesse and a farmer resident there received EU funds from the EAGF and EAFRD. The defendant's website published the name and address of beneficiaries,

plus annual amounts received, in accordance with Regulation 1290/2005 (rules on financing of expenditure falling under CAP) and Regulation 259/2008 (requiring publication exclusively on the internet). The applicants filed an action in national court to prevent publication of data relating to them.

Question referred: Whether provisions requiring publication of this data on the internet are valid and consistent with data protection requirements.

Legal persons: Legal persons can claim protection of Articles 7 and 8 of the CFR only insofar as the official title of the legal person identifies one or more natural persons. Here, the name of the legal person directly identifies the natural persons who are its partners. (¶ 53)

Consent: The legislation at issue does not seek to base the personal data processing for which it provides on consent of the beneficiaries concerned. Rather, it provides that they are to be informed. Thus, processing is not based on their consent. Therefore, it is necessary to analyse whether interference is justified under Article 52(1) of the CFR. (¶ 54)

Articles 7/8 CFR: The validity of legislation requiring publication must be assessed in light of provisions of the CFR, including Article 8. However, CFR Article 52(1) accepts that limitations may be imposed on rights under the CFR, as long as they are provided by law, respect the essence of those rights and are proportionate (necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.) Further, CFR Article 52(3) states that for rights in the CFR which correspond to rights in the ECHR, the meaning and scope shall be same as that given in the ECHR. (¶¶ 46-51)

Publication on the website of data naming beneficiaries and amounts they receive constitutes interference with private life under Article 7 of the CFR. It is irrelevant that the data concerns activities of a professional nature, as under Article 8 ECHR, the CFR has held that no principle justifies exclusion of activities of a professional nature from the notion of private life. (¶¶ 58-59)

Publication must a) be provided by law, b) respect the essence of the rights and freedoms in Articles 7 and 8 of the CFR, and c) be proportionate (necessary and genuinely meet the objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others). Here, publication is lawful since it is specifically provided for by the Regulation. It meets the general interest requirement because publication is intended to enhance transparency regarding use of CAP funds and sound financial management. Regarding proportionality, it is necessary to analyse whether the EU balanced its interest in guaranteeing transparency and ensuring the best use of public funds with the rights of beneficiaries to privacy and data protection. Derogations to data protection are allowed only insofar as they are strictly necessary. (¶¶ 66-77)

- For natural persons, there is nothing to show that lawmakers made an effort to strike a balance. No automatic priority can be conferred on the objective of transparency over data protection, even if important economic interests are at stake. Thus, the lawmaker exceeded the limits which the proportionality principle imposes. (¶¶ 80-85)

- Publication of the data in question with respect to the complainant legal person does not go beyond limits imposed by the proportionality principle. The seriousness of the breach manifests itself in different ways for legal persons versus natural persons. It would impose an unreasonable administrative burden on the competent national authorities if they were obliged to examine, before the data are published for each legal person who is a beneficiary, whether the name of that person identifies natural persons. Thus, the legislation requiring publication is valid with respect to the legal persons. (¶¶ 87-88)

1.14. CASE C-70/10, SCARLET EXTENDED SA V. SOCIETE BELGE DES AUTEURS, COMPOSITEURS ET EDITEURS SCRL (SABAM), 24.11.2011 ("SCARLET")

Reference for a preliminary ruling by the cour d'appel de Bruxelles (Belgium). SABAM, a management company representing authors, composers and editors of musical works, brought proceedings in the Belgian court against Scarlet, an internet service provider (ISP), to take measures to bring an end to copyright infringements committed by Scarlet's customers. Scarlet had been ordered by the Belgian court of first instance to install a system for filtering electronic communications which use file-sharing software ("peer-to-peer"), with a view to preventing file

sharing which infringes copyright. Scarlet appealed. The court of appeal referred the question for preliminary ruling.

Question referred: Whether EU Directives on electronic commerce in the internal market, intellectual property rights and data protection, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be construed as precluding an injunction on an ISP to introduce such a filtering system.

Definition of personal data: ISP addresses are protected personal data because they allow the concerned users to be precisely identified. (¶ 51)

Necessity/proportionality: The contested filtering system may infringe the right to protection of personal data of the ISP's customers, as it would involve a systematic analysis of all content and the collection and identification of the users' IP address from which unlawful content on the network is sent. (¶¶ 50-51)

Balancing fundamental rights: The injunction to install the contested filtering system did not respect the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information. (¶ 53)

1.15. CASE C-461/10, BONNIER AUDIO AB ET AL. V. PERFECT COMMUNICATION SWEDEN, 19.4.2012 ("BONNIER")

Reference for a preliminary ruling by the Högsta domstolen (Sweden). The applicants, which are publishing companies that hold copyrights to 27 audiobooks, brought proceedings in the Swedish court for copyright infringement by means of a file transfer protocol (FTP) server which allows file sharing and data transfer via the internet. The applicants applied to the Swedish court for an order for the disclosure of the name and address of the person using the IP address from which the files were sent. EPhone, the ISP, challenged the application, alleging that it violated the Data Retention Directive.

Questions referred: (1) Whether Directove 2006/24 precludes the application of a national provision which permits an internet service provider in civil proceedings, in order to identify a particular subscriber, to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided a specific IP address, which it is claimed was used in the infringement; (2) whether the answer to the first question is affected by the fact that the Member State has not implemented Directive 2006/24.

Scope of Directive 2006/24: Directive 2006/24 deals exclusively with the handling and retention of data generated by electronic communication service providers for the purpose of the investigation, detection, and prosecution of serious crime and their communication to competent national authorities. Thus, a national provision transposing the EU intellectual property directive, which permits an ISP in civil proceedings to be ordered to give a copyright holder information on the subscriber to whom the ISP provided an IP address allegedly used in an infringement, is outside the scope of Directive 2006/24 and therefore not precluded by that Directive. It is irrelevant that the Member State concerned has not yet transposed Directive 2006/24. (¶¶ 40-41)

Definition of processing: Communication of the name and address sought by applicants constitutes processing of personal data. (¶ 52)

Scope of Directive 2002/58: The communication of the name and address in question falls within the scope of Directive 2002/58 (and within the scope of Directive 2004/48, dealing with copyright). (¶¶ 52-54)

Balancing fundamental rights: The national legislation in question requires, for an order for disclosure of the data in question to be made, that there be clear evidence of an infringement of an intellectual property right, that the information can be regarded as facilitating the investigation into a copyright infringement and that the reasons for the measure outweigh the potential harm to the person affected. Thus, it enables the national court seised of an application for an order for disclosure of personal data to weigh the conflicting interests involved, and thereby in principle ensures a fair balance between protection of intellectual property rights and protection of personal data. (¶¶ 58-60)

1.16. JOINED CASES C-468/10 AND C-469/10, ASOCIACION NACIONAL DE ESTABLECIMIENTOS FINANCIEROS DE CREDITO (ASNEF) AND FEDERACION DE COMERCIO ELECTRONICO Y MARKETING DIRECTO (FECEMD) V. ADMINISTRACION DEL ESTADO, 24.11.2011 ("ASNEF")

Reference for a preliminary ruling by the Tribunal Supremo of Spain. The applicants in national proceedings challenged the validity of Royal Decree 1720/2007 implementing Organic Law 15/1999. These national rules provide that, in the absence of the interested party's consent, and to allow processing of his personal data that is necessary to pursue a legitimate interest of the controller or recipients, it is necessary not only that the fundamental rights and freedoms of the data subject should not be prejudiced, but also that the data should appear in public sources. These requirements go beyond the provisions of Article 7(f) of Directive 95/46.

Questions referred: Whether a Member State can add new principles relating to the lawfulness of processing of personal data to those specified in Article 7 of Directive 95/46 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7; Whether Article 7(f) has direct effect.

Transposition/harmonisation: Harmonisation of national laws is not limited to minimal harmonisation but harmonisation which is generally complete. Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of data subjects, equivalent in all Member States. Consequently, Article 7 of Directive 95/45 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as lawful. That interpretation is corroborated by the term "may be processed only if", which demonstrates the exhaustive and restrictive nature of the list appearing in that Article. Thus, the Member States cannot add new principles relating to the lawfulness of processing or impose additional requirements. (¶¶ 29-32)

Article 5 authorises Member States to specify the conditions under which the processing of personal data is lawful, within the limits of Article 7, *inter alia*. That margin of discretion can be used only in accordance with the objective pursued by the Directive of maintaining a balance between the free movement of personal data and the protection of private life. A distinction must be made between national measures that provide for additional requirements amending the scope of a principle referred to in Article 7 (precluded) and national measures which provide for a mere clarification of one of those principles (allowed). Thus, Article 7(f) precludes any national rules which, in the absence of the data subject's consent, impose requirements that are additional to the two cumulative conditions set out in that Article. (¶¶ 33-39)

Balancing fundamental rights: The second condition of Article 7(f) (the interests of the controller or recipients must not be overridden by the fundamental rights and freedoms of the data subject) necessitates a balancing of the opposing rights and interests concerned, which depends on the individual circumstances of the particular case. In relation to the balancing, it is possible to take into consideration the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources. The processing of data appearing in non-public sources necessarily implies that information relating to the data subject's private life will thereafter be known by the data controller and recipients, which is a more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights, and must be properly taken into account in the balancing. However, it is no longer a precision within the meaning of Article 5 if national rules exclude the possibility of processing certain categories of personal data by definitively prescribing the result of the balancing thereby not allowing a different result by virtue of the particular circumstances of an individual case. (¶¶ 40-47)

Direct applicability: Whenever the provisions of a Directive appear to be unconditional and

sufficiently precise, they have direct effect if the Member State has failed to implement that Directive in domestic law by the end of the prescribed period. Article 7(f) is sufficiently precise, as it states an unconditional obligation. (¶¶ 52-55)

1.17. C-614/10, COMMISSION V. AUSTRIA, 16.10.2012 ("AUSTRIA")

Infringement procedure against Austria, alleging that it incorrectly transposed the second paragraph of Article 28(1) of Directive 95/46 (the requirement for an independent Data Protection Authority (DPA)), insofar as the national legislation does not allow the Data Protection Commission (DSK) to exercise its functions "with complete independence."

Independence of DPA: By failing to take all measures necessary to ensure that the Austrian national legislation meets the requirement of independence with regard to the DSK, Austria has failed to fulfill its obligations under the second subparagraph of Article 28(1) of Directive 95/46 and Article 8(3) of the EU Charter of Fundamental Rights and Article 16(2) TFEU. The establishment in Member States of independent supervisory authorities is thus an essential component of the protection of individuals with regard to the processing of personal data.

The words "with complete independence" must be given an autonomous interpretation. Supervisory authorities must enjoy an independence with allows them to perform their duties free from external influence, direct or indirect, which is liable to have an effect on their decisions. The fact that DSK has functional independence insofar as its members are "independent and [are not] bound by instructions of any kind in the performance of their duties" is an essential, but not sufficient, condition to protect it from all external influence. (¶¶ 41-42)

Here, the national legislation provides only for the operational autonomy of the supervisory authority, but does not preclude the DSK from performing its duties free from all indirect influence, for the following reasons:

(1) The managing member of the DSK need not always be an official of the Federal Chancellery (although it always has been), and all day-to-day business is thus *de facto* managed by a federal official, who remains bound by the instructions issued by his employer and is subject to supervision. It is conceivable that the evaluation of the managing member by his hierarchical superior for the purposes of encouraging his promotion could lead to a form of "prior compliance". Moreover, the Chancellery is subject to the supervision of the DSK, so the DSK is not above all suspicion of partiality. The service-related link between the managing member of the DSK and the Chancellery affects the DSK's independence. The fact that the appointment of the managing member rests on an autonomous decision of the DSK does not protect the independence of the supervisory authority; (¶¶ 45-55)

(2) The office of the DSK is structurally integrated with the departments of the Federal Chancellery, and all DSK staff are under the authority of the Federal Chancellery and subject to its supervision. The DSK need not be given a separate budget to satisfy the criterion of independence. They can provide that the DPA comes under a specified ministerial department. However, the attribution of the necessary equipment and staff to DPAs must not prevent them from acting with complete independence. Here, since they are subject to supervision by the Chancellery, it is not compatible with the requirement of independence. (¶¶ 56-61)

(3) The Federal Chancellor has the right to be informed of all aspects of the work of the DSK. This precludes the DSK from operating above all suspicion of partiality. (¶¶ 62-63)

1.18. C-119/12, PROBST V. MR.NEXNET GMBH, 22.11.2012 ("PROBST")

Reference for a preliminary ruling by the Bundesgerichtshof, Germany. The applicant (Probst) is the recipient of internet services supplied by Verizon through, and billed by, Deutsche Telecom. The respondent (mr.nexnet) is the assignee of claims for payment for the supply of internet services by Verizon. The applicant failed to pay some of the charges. The contract between legal predecessors of the respondent and Verizon provided that personal data would be processed exclusively for the purpose of that contract, and deleted immediately thereafter.

Questions referred: Whether Directive 2002/58 permits the passing of traffic data from the

service provider to the assignee of a claim for payment in respect of telecommunications services in the case where the assignment effected with a view to the collection of transferred debts includes, in addition to the general obligation to respect the privacy of telecommunications and to ensure data protection as provided for under the applicable legislation, contractual stipulations that: (1) the service provider and assignee undertake to process the personal data only within the framework of their cooperation and exclusively for the purpose of the contract; (2) as soon as the data is no longer required for such purpose, the data will be erased or returned; (3) each contracting party is entitled to check that the other has ensured data protection and security in accordance with the agreement; (4) confidential documents and information transferred may be made accessible only to such employees as required for purposes of performing the contract; (5) those employees are required to maintain confidentiality; (6) on request or termination of the cooperation between the contracting parties, the data will be erased or returned.

Traffic data: Article 6(2) of Directive 2002/58 provides an exception to the confidentiality of communications, stating that traffic data necessary for purposes of subscriber billing and interconnection payments may be processed "up to the end of the period during which the bill may lawfully be challenged or payment pursued." Thus, the provision covers the processing necessary for securing payment, including debt collection. (¶ 17)

Article 6(5) provides that traffic data processing authorized by Article 6(2) "must be restricted to persons acting *under the authority of* [the service] providers of the public communications networks and publicly available electronic communications services handling billing" and "must be restricted to what is necessary" for the purpose of such activity. Thus, the assignee of claims for payment is authorized to process the data on condition that it acts "under the authority" of the service provider and that it processes only traffic data which are necessary for the purpose of recovery of those claims. That provision seeks to ensure that such externalization of debt collection does not affect the level of protection of personal data enjoyed by the user. "Under the authority" must be strictly construed to mean that the assignee acts only on instructions and under the control of the service provider. The contract between the service provider and assignee must contain provisions ensuring the lawful processing of traffic data by the assignee and must allow the service provider to ensure at all times that those provisions are being complied with by the assignee. (¶¶ 18-27)

1.19. C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 ("GOOGLE")

Reference for a preliminary ruling by the Audiencia Nacional (Spain). Mr. G, a Spanish national resident in Spain, sued Google Spain, Google Inc. and La Vanguardia newspaper, alleging that when an internet user entered his name in the Google search engine, he would obtain links to two pages of La Vanguardia newspaper on which an announcement with his name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts. He requested *inter alia* that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. The DPA granted the request against Google Spain and Google Inc. Information indexed by Google Search following the location and sweeping of websites throughout the world by its web crawlers is stored temporarily on servers whose state of location is unknown. Google provides results with advertising associated with the user's search terms. The subsidiary Google Spain promotes the sale of advertising in Spain, and was registered as the controller of related processing in Spain.

Questions referred: (1) Whether an "establishment" exists where one or more of the following circumstances arises: the undertaking providing the search engine sets up in a Member State an office or subsidiary to promote and sell advertising space on the search engine, or when the parent designates a subsidiary in that Member State as its representative and controller for two specific filing systems which relates to the data of customers who have contracted for advertising, or when the office or subsidiary forwards to the parent, located outside the EU, requests and requirements addressed to it both by data subjects and DPAs; (2) Whether there is a "use of equipment …situated on the territory of the said Member State" under Article 4(1)(c) of Directive 95/46 when a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State or when it uses a domain name pertaining to a Member State and arranges for searches and the results to be based on the language of that Member State; (3) Whether the temporary storage of the information indexed by internet search engines is a "use of equipment" under Article 4(1)(c); (4) Whether Directive 95/46 must be applied, in light of

Article 8 of the CFR, in the Member State where the centre of gravity of the conflict is located; (5) Does the activity of Google Search fall within the concept of processing in Article 2(b) of Directive 95/46; (6) Whether the undertaking managing Goggle Search is a controller of the personal data contained in the web pages that it indexes; (7) Whether the DPA can directly impose on Google Search a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located; (8) Whether the obligation of search engines to protect those rights would be excluded when the personal data has been lawfully published by third parties and is kept on the web page from which it originates; (9) Whether the rights of erasure, blocking and objection of Directive 95/46 extend to enabling the data subject to address himself to search engines in order to prevent indexing of the data, published on the third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though it has been lawfully published by third parties.

Definition of processing: The operation of loading personal data on an internet page must be considered processing (as the court held in Lindquist). In exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine "collects" such data which it subsequently "retrieves", "records" and "organizes" within the framework of its indexing programmes, "stores" on its servers and, as the case may be, "discloses" and "makes available" to its users in the form of lists of search results, which constitute processing, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data. This finding is not affected by the fact that those data have already been published on the internet and are not altered by the search engine. It is not necessary that the personal data be altered. While alteration of personal data constitutes processing under Article 2(b), the other operations mentioned there do not require the alteration of personal data.

The processing done by the search engine operator is distinguished from and in addition to that done by publishers of websites, consisting in loading those data on an internet page. (¶¶ 26-31)

Definition of controller: The search engine operator determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of the activity and is thus a controller. It would be contrary not only to the clear wording of Article 2(d) and to its objective, which is to ensure through a broad definition of the concept of controller, effective and complete protection of data subjects, to exclude the operator of a search engine on the ground that it does not exercise control over the personal data published on the web pages of third parties. Moreover, the activity of search engines plays a decisive role in the overall dissemination of the personal data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published. The search results also provide a structured overview of the information relating to that individual that can be found on the internet, enabling them to establish a detailed profile of the data subject. The fact that publishers of websites have the option of indicating to operators by means of exclusion protocols that they wish some information published on their site to be excluded from the search engines' automatic indexing does not mean that if publishers do not so indicate, the operator of the search engine is released from responsibility for its processing of personal data. (¶¶ 33-41)

Scope of Directive 95/46:

- Google Spain is an "establishment" within the meaning of Article 4(1)(a). It engages in the effective and real exercise of activity through stable arrangements in Spain, and is a subsidiary of Google Inc. on Spanish territory. (¶ 49)

- The processing of personal data by the controller is also "carried out in the context of the activities" of an establishment, even though Google Spain is not involved in the processing at issue (which is carried out exclusively by Google Inc.) but rather only in advertising in Spain. Article 4(1)(a) does not require that the processing in question be carried out "by" the establishment concerned, but only "in the context of the activities" of the establishment. In light of the objective of effective protection of fundamental rights, those words cannot be interpreted restrictively. The activities of the search engine and those of its establishment in the Member State are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine economically profitable and that engine is the means

enabling those activities to be performed. (¶¶ 52-56, 60)

Data subject rights: The non-compliant nature of processing may arise from the breach of any conditions of lawfulness imposed by the Directive, including data quality and legitimacy. Here, the grounds for legitimacy were those specified in Article 7(f), which permits processing where necessary for the purposes of the legitimate interests pursued by the controller or third party to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights of the data subject. This requires a balancing of interests. Balancing provided in Article 14 allows account to be taken of all circumstances surrounding the data subject's particular situation. (¶¶ 70-75)

- Interest of the data subject: The search of the individual's name enables any internet user to obtain, through a list of results, a structured overview of the information relating to that data subject that can be found on the internet. This may potentially concerning a vast number of aspects of his private life enabling a detailed profile. Without the search engine, this data could not have been interconnected or only with great difficulty. The interference with the rights of the data subject is heightened because of the important role played by the internet and search engines in modern society. (¶ 80)

- The interests of the search engine: These are economic interest, which cannot justify the potential seriousness of the interference with the data subject's rights. (¶ 81)

- Interests of the internet users: The data subjects' rights generally override those of internet users, but the balance may depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, which may vary by the role played by the data subject in public life. The interference may be justified by the preponderant interests of the general public in having access to the information. (¶ 81)

- The Supervisory authority or judicial authority may order the search engine operator to remove the link from the list of results without presupposing the previous or simultaneous removal of the underlying information from the web page on which it was published. Requiring the data subject to obtain erasure from web pages would not provide effective and complete protection of data subject, especially because publishers may not be subject to EU data protection law or publication may be carried out "solely for journalistic purposes" and thus benefit from derogation. Further, balancing would be different for processing by the search engine and processing by the web publisher. (¶¶ 82-85)

Right of erasure: The search engine operator must erase information and links concerned in the list of results if that information appears, having regard to all circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine. Here, having regard to the sensitivity for data subject's private life of information contained in announcements and the fact that the initial publication occurred 16 years earlier, the data subject has established that the links should be removed. (¶ 98)

1.20. C-141/12 AND C-372/12, MINISTER VOOR IMMIGRATIE V. M, 17.7.2014 ("M")

Reference for a preliminary ruling by the Rechtbank Middelburg and the Raad van State. Several third country nationals applied for a residence permit for a fixed period in the Netherlands. One applicant asked for a residence permit for a fixed period which was denied, the other asked for the same which was granted. Both asked for a copy of the minute which explained the decision, and both were denied access.

Questions referred (partial listing): (1) Whether the second indent of Article 12(a) of Directive 95/46 should be interpreted to mean that there is a right to a copy of documents in which personal data have been processed, or is it sufficient if a full summary, in an intelligible form, of such data is provided; (2) Whether the words "right of access" in Article 8(2) CFR should be interpreted to mean there is a right to a copy of documents; (3) Whether a legal analysis, as set out in a "minute", can be regarded as personal data; (4) Whether protection of the rights and freedoms of

others under Article 13(1)(g) of Directive 95/46 can cover the interest in an internal undisturbed exchange of views within the public authority concerned.

Definition of personal data: The data relating to the applicant for a residence permit included in the minute (applicant's name, DOB, nationality, gender, ethnicity, religion and language) constitute personal data. The legal analysis in the minute may contain personal data but it does not in itself constitute such data. The legal analysis is not information relating to the applicant, but at most, in so far as not limited to a purely abstract interpretation of the law, is information about the assessment and application by the competent authority of that law to the applicant's situation. This interpretation is consistent with the language of Article 2(a) and the objective and general scheme of Directive 95/46. (¶¶ 34, 38-41)

Right of access: Regarding the right of access, protection of the fundamental right to respect for private life means that the data subject may be certain that the personal data concerning him are correct and that they are processed lawfully. It is in order to carry out the necessary checks that the data subject has, under Article 12(a), a right of access, which is necessary to obtain rectification, erasure or blocking of his data (Article 12(b)). The legal analysis is not in itself liable to be the subject of a check of its accuracy by the applicant and rectification, while the facts are. Moreover, the right of access is not designed to ensure the greatest possible transparency of the decision-making process of public authorities and to promote good administrative practices (as is the case for the right of access to documents). (¶¶ 44-46)

To comply with the right of access under Article 12(a) and Article 8(2) of CFR, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with the Directive. He need not be given a copy of the documents. (¶¶ 59-60)

1.21. C-288/12, COMMISSION V. HUNGARY, 8.4.2014 ("HUNGARY")

Infringement procedure against Hungary for failure to fulfil obligations under Article 258 TFEU. Mr. J was appointed for 6 years as DPA. However, pursuant to transitional measures related to revision of data protection law, Hungary prematurely ended his term and appointed a new DPA for 9 years.

Independence of DPA: Establishment in a Member State of an independent supervisory authority is an essential component of the protection of individuals with regard to the processing of personal data. Operational independence of supervisory authorities, in that members are not bound by instructions of any kind in the performance of their duties, is an essential condition that must be met to respect the independence requirement, but this is not sufficient. The mere risk that the state could exercise political influence over decisions of a supervisory authority is enough to hinder independence. If it were permissible for the Member State to compel the supervisory authority to vacate office before serving his/her full term, even if this comes about as a result of restructuring or changing of the institutional model, the threat of such premature termination could lead the supervisory authority to enter into a form of prior compliance with the political authority. This is incompatible with the requirement of independence, and the supervisory cannot be regarded as being able to operate above all suspicion of partiality. Member States are free to adopt or amend the institutional model they consider most appropriate for supervisory authorities. However, they must ensure that the independence of the authority is not compromised, which entails the obligation to allow that authority to serve his/her full term. (¶¶ 51-55, 60)

1.22. C-291/12, SCHWARZ V. BOCHUM, 17.10.2014 ("SCHWARZ")

Reference for a preliminary ruling by the Verwaltungsgericht Gelsenkirchen (Germany). Applicant applied to Stadt Bochum for a passport, but refused to have his fingerprints taken, and Stadt therefore refused his application. He brought an action before the referring court to have a passport issued without taking his fingerprints.

Questions referred (partial listing): Is Article 1(2) of Regulation 2252/2004 to be considered valid, on the ground that it breaches certain fundamental rights of the holders of passports issued in accordance with that provision.

Definition of personal data: Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows them to be identified with precision. (¶ 27)

Definition of processing: Taking and storing fingerprints constitute processing. (¶¶ 28-29)

Articles 7 and 8 CFR: Taking and storing of fingerprints by national authorities, governed by Article 1(2) of Regulation 2252/2004, constitute a threat to the rights of respect for private life and protection of personal data. (¶ 30)

Article 52(1) allows for limitations on exercise of rights in Articles 7 and 8 CFR as long as limitations are provided for by law, respect the essence of those rights, and respect proportionality (necessary and genuinely meet objectives of general interest recognised by EU or need to protect rights and freedoms of others). Here, taking of fingerprints for passports is provided by Regulation 2252/2004 to prevent falsification of passports and fraudulent use thereof, and illegal entry into the EU. Therefore, the provision pursues an objective of general interest recognised by the EU. (¶¶ 34-38)

Consent: It is essential for citizens of the EU to own a passport in order to travel to a third country, and a passport must contain fingerprints. Therefore, citizens are not free to object to processing of their fingerprints, and thus persons applying for passports cannot be deemed to have consented to that processing. (¶ 32)

Necessity/proportionality: Storage of fingerprints on a highly secure storage medium is likely to reduce risk of passports being falsified and to facilitate the work of the authorities responsible for checking the authenticity of passports at EU borders, although it is not wholly reliable. Thus, it is appropriate. (¶¶ 41-45)

The action involves taking prints of two fingers, causing no physical or mental discomfort, plus a facial image. The only real alternative to fingerprints is iris scan, the technology of which is not yet as advanced as fingerprint recognition. Thus, there is no apparent alternative that is sufficiently effective and less of a threat to the protected rights. (¶¶ 48-53)

The concern that data may be centrally stored and used for other purposes (e.g. criminal investigation or monitor the person indirectly) does not affect the validity of the Regulation, which provides only for preventing illegal entry into EU. (¶¶ 61-62)

1.23. C-293/12 AND C-594-12, DIGITAL RIGHTS IRELAND LTD V. IRELAND, 8.4.2014 ("DRI")

Reference for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof (Austria). Digital Rights Ireland brought an action in High Court claiming that it owned a mobile phone which it used since 2006, challenging national measures requiring retention of data relating to electronic communications and asking the court to declare the invalidity of Directive 2006/24, which requires telephone communications service providers to retain traffic and location data for a period specified by national law to prevent, detect, investigate and prosecute crime and safeguard security.. This data that which is necessary to trace and identify the source of a communication and its destination, the date, time, duration and type of a communication, users' communication equipment, and location of mobile equipment including name and address of subscriber, calling telephone number, number called and IP address for internet users.

The directive does not permit the retention of content, but it might have an effect on the use of the means of communication and consequently on the exercise of freedom of expression guaranteed by Article 11 CFR. It also directly affects private life (guaranteed by Article 7 CFR) and constitutes processing of personal data (therefore falls under Article 8 CFR).

Articles 7 and 8 CFR: The obligation on providers of publicly available electronic communications services or public communications networks to retain data relating to a person's private life and his communications in itself constitutes an interference with Article 7. Access of competent national authorities to the data constitutes a further interference with that right. The Directive constitutes an interference with Article 8 because it provides for processing of personal data. These interferences with Articles 7 and 8 are wide-ranging and particularly serious. The fact that data are

retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of users the feeling that their private lives are the subject of constant surveillance. (¶¶ 29, 32, 34-37)

Any limitation on the exercise of rights and freedoms laid down by CFR must be provided by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet the objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others. Even though retention constitutes a particularly serious interference with the right to privacy, it is not such as to adversely affect the essence of those rights given that the Directive does not permit the acquisition of knowledge of the content of the electronic communications. Nor does it adversely affect the essence of the right to protection of personal data because certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or public communications networks, in order to ensure appropriate technical and organizational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data. (¶¶ 38-40)

Directive 2006/24: The material objective of the Directive is of general interest – to ensure that data are available for the purpose of the investigation, detection and prosecution of serious crime, and therefore to public security, and international terrorism. (Article 6 CFR lays down the right of any person to liberty and security.) Data relating to use of electronic communications are particularly important and a valuable tool in prevention of offences and the fight against crime. (¶¶ 41-44)

Necessity/proportionality: The principle of proportionality requires that acts of EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation and do not exceed the limits of what is appropriate and necessary to achieve those objectives. Here, given the important role played by data protection in light of the fundamental right of privacy, and the extent and seriousness of the interference, the EU legislature's discretion is reduced, thus the review of that discretion should be strict. Retention of data is an appropriate tool for the objective pursued. (¶¶ 46-49)

The fight against serious crime and terrorism is of the utmost importance to ensure public security and its effectiveness may depend on the use of modern investigation techniques. But this does not, in itself, justify the necessity of the retention measure. Derogations and limitations in relation to data protection must apply only insofar as strictly necessary. Here, the legislation must lay down clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees effectively to protect their personal data against the risk of abuse, and unlawful access and use of the data. The need for safeguards is all the greater where personal data are subjected to automatic processing and there is significant risk of unlawful access to the data. Further, the Directive requires retention of all traffic data concerning fixed telephony, mobile telephony, internet access, internet e-mail and internet telephony – i.e. all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. This covers all subscribers and registered users, and therefore entails an interference with the fundamental rights of practically the entire European population, without a need for a link to crime. (¶¶ 51-58)

Lawfulness: The Directive fails to lay down objective criteria by which to determine the limits of access of competent national authorities to the data and its use, nor substantive and procedural conditions relating to access by competent national authorities and to their subsequent use. It does not lay down objective criteria to limit the number of persons authorized to have access and use to what is strictly necessary, and it is not made dependent on prior review carried out by a court or independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of obtaining the objective pursued. (¶ 62)

Retention: The Directive establishes a retention period of a minimum of 6 months and a maximum of 24 months, but it is not stated that determination of this period must be based on objective criteria to ensure that it is limited to what is strictly necessary. (¶¶ 63-64)

Security: The Directive does not provide for sufficient safeguards to ensure effective protection of the data retained against risk of abuse and unlawful access. It does not lay down rules adapted to the vast quantity of data whose retention is required, the sensitive nature of that data, and the risk

of unlawful access, nor is there a specific obligation set on Member States to establish such rules. Rather, it permits providers to have regard to economic considerations when determining the level of security. (¶¶ 66-67)

Supervision: The Directive does not require that the data be retained within the EU, with the result that it cannot be held that the control by an independent authority of compliance with the requirements of data protection and security is fully guaranteed. This is an essential component of protection of individuals with regard to the processing of personal data. (¶ 68)

Necessity/proportionality: Accordingly, the EU legislature exceeded limits imposed by compliance with principle of proportionality in light of Articles 7, 8 and 52(1) CFR. (¶ 69)

1.24. C-342-12, WORTEN-EQUIPAMENTOS PARA O LAR SA V. ACT (AUTHORITY FOR WORKING CONDITIONS), 30.5.2013 ("WORTEN")

Reference for a preliminary ruling from Tribunal do Trabalho de Viseu (Portugal). Worten (a private company in Portugal) adopted a system of restricted access to working hour records of staff, which did not allow ACT to have automatic access. ACT considered this a serious offence of national law on workers and imposed a fine.

Questions submitted: (1) Whether the record of working time for each worker is covered by the concept of personal data under Article 2 of Directive 95/46; (2) If so, whether the Portugese state is obliged to provide appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network; (3) When the Member State does not adopt any such measure, and the employer as controller does not allow automatic access by the national authority responsible for monitoring working conditions, whether the principle of the primacy of European law is to be interpreted to mean that the Member State cannot penalize the employer for that action?

Personal data definition: Data contained in a record of working time concerning, in relation to each worker, the daily work periods and rest periods, constitute personal data because they represent "information relating to an identified or identifiable natural person. (¶ 19)

Security: Article 17(1) requires controllers (not Member States) to adopt technical and organizational measures which, having regard to the state of the art and cost of their implementation, are to ensure a level of security appropriate to the risks represented. The obligation under national law to provide the national authority responsible for monitoring working conditions with immediate access to the record of working time does not imply the data must be made accessible to persons not authorised for that purpose (as Worten claimed). Rather, Worten must ensure that only those persons duly authorised to access the personal data in question are entitled to respond to a request for access from a third party. Thus, Article 17(1) is not relevant here. (¶¶ 24-25, 28-29)

Necessity/proportionality: The referring court must verify that the personal data contained in the record of working time are collected in order to ensure compliance with the national legislation relating to working conditions, that the processing of those data is necessary for compliance with a legal obligation to which Worten is subject and the performance of the monitoring task entrusted to the national authority responsible for monitoring working conditions. Only the grant of access to authorities having powers of monitoring could be considered to be necessary within the meaning of Article 7(e). Further, the obligation to provide immediate access to the record could be necessary if it contributes to the more effective application of the legislation relating to working conditions. It is for referring court to decide whether this requirement is necessary. (¶¶ 35-43)

Proportionality: Penalties must respect the principle of proportionality. (¶ 44)

1.25. C-473/12, IPI V. ENGLEBERT ("ENGLEBERT")

Reference for a preliminary ruling by the Belgian constitutional court. The applicant is responsible for ensuring compliance with conditions of access to and proper practice of the profession of estate agent. It asked the Charleroi commercial court to declare that defendants had violated applicable rules and should cease various estate agency activities, based on facts gathered

by private detectives. The question arose whether the private detectives had acted in breach of national data protection provisions, because they had not informed defendants before collecting their data (Article 10 of Directive 95/46), or third parties at the time of collection of the data (Article 11 of Directive 95/46).

Questions referred: (1) Whether Article 13(1)(g) leaves the Member States free to choose whether to provide for an exception to the immediate obligation to inform set out in Article 11(1) if this is necessary in order to protect the rights and freedoms of others, or are the Member States subject to restrictions in this matter; (2) Whether the professional activities of private detectives, governed by national law and exercised in the service of authorities authorized to report to judicial authorities any infringement of the provisions protecting a professional title and organizing a profession, comes within the exception in Article 13(1)(d) and (g); (3) Whether that Article is compatible with Article 6(3) TEU, the principle of equality and non-discrimination.

Definition of personal data: Data collected by private detectives relating to persons acting as estate agents concern identified or identifiable natural persons, and therefore constitute personal data. (¶ 26)

Transposition/harmonisation: Article 13(1) states "Member States may" and thus does not oblige the Member States to lay down in their national law exceptions for the purposes listed therein. Rather, they have the freedom to decide whether, and for what purposes, to take legislative measures aimed at limiting the extent of the obligations to inform the data subject. Further, they may take such measures only when necessary. (¶ 32)

Derogations: The activity of a body such as IPI (a professional body responsible for ensuring compliance with the rules governing the profession of estate agent which is a regulated profession in Belgium, through investigating and reporting breaches of those rules) corresponds to "the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions" and is capable of coming under that exception. The directive does not prevent such a professional body from having recourse to private investigators. Thus, if a Member State has chosen to implement the exception, then the professional body and private detectives may rely on it and are not subject to the obligation to inform the data subject. However, if the Member State has not implemented the exception, the data subjects must be informed. (¶¶ 42-46)

Rules on access to a regulated profession form part of the rules of professional ethics, therefore investigations concerning the acts of persons who breach those rules by passing themselves off as estate agents are covered by the exception in Article 13(1)(d). (¶ 50)

1.26. C-486/12, X, 12.12.2013 ("X")

Reference for a preliminary ruling by the Gerechtshof te 's-Hertogenbosch (Netherlands). X requested her municipality to disclose her various addresses in 2008 and 2009 to prove that she had not received notices requesting payment of a fine for a traffic violation. The municipality responded with a certified transcript, demanding payment of a fee of EUR 12,80.

Questions referred: (1) Whether the provision of access to data pursuant to a provision under national law constitutes compliance with the obligation to communicate data undergoing processing (Article 12(a) of Directive 95/46); (2) Whether Article 12(a) precludes the levying of fees in respect of the communication, by means of a transcript from the municipal database, of personal data undergoing processing; (3) Whether the levying of the present fee is excessive.

Access: Article 12(a) of Directive 95/46 does not require Member States to levy fees when the right of access to personal data is exercised, nor does it prohibit the levying of such fees as long as they are not excessive. Access must be without constraint, without excessive delay and without excessive expense. The fees should be fixed at a level which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular his right to have the data communicated to him in an intelligible form, and on the other, the burden which the obligation to communicate such data represents for the controller. The fees may not be fixed at a level likely to constitute an obstacle to the exercise of the right of access, and it should not exceed the cost of communicating such data. (¶¶ 22, 25, 28-30)

1.27. C-212/13, RYNES V. ÚŘAD PRO OCHRANU OSOBNICH ÚDAJŮ, 11.12.2014 ("RYNES")

Reference for a preliminary ruling by the Nejvyšší správní soud (Czech Republic). The applicant (a private individual) installed and used a video camera system located under the eaves of his home, which recorded the entrance to his home, the public footpath and the entrance to the house opposite. The purpose was to protect the property, health and life of his family and himself, as they had been subjected to attacks by persons unknown whom it had not been possible to identify. A further attack took place which was recorded, and the recording made it possible to identify two suspects. The applicant provided the recording to the police who relied on it in subsequent criminal proceedings.

Question referred: Whether the operation of a camera system installed on a family home for the purposes of the protection of the property, health and life of the owners of the home can be classified as the processing of personal data "by a natural person in the course of a purely personal or household activity" for the purposes of Article 3(2) of Directive 95/46, even though such a system also monitors public space.

Definition of personal data: The image of a person recorded by a camera constitutes personal data because it makes it possible to identify the person concerned. (¶ 22)

Definition of processing: Video surveillance involving the recording and storage of personal data falls within the scope of the Directive, since it constitutes automatic data processing. (¶ 24)

Processing for purely personal or household activity: Protection of the fundamental right to private life guaranteed under Article 7 of the CFR requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. Also, the wording of the derogation refers to "purely" personal or household activity, not simply a personal or household activity. Correspondence and the keeping of address books constitute, in the light of recital 12 to Directive 95/46, a purely personal or household activity, even if they incidentally concern the private life of other persons. However, to the extent that the video surveillance covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data, it cannot be regarded as a purely personal or household activity. Thus, the consent of the data subject would be required to process his data. (¶¶ 28-35)

Definition of controller: Arts. 7(f), 11(2) and 13(1)(d) and (g) make it possible to take into account the legitimate interests of the controller in protecting the property, health and life of his family and himself. (¶ 34)

1.28. C-615/13 P, CLIENT EARTH ET AL. V. EFSA, 16.7.2015 ("CLIENT EARTH")

Appeal from a judgment of the General Court dismissing an action for annulment of a decision of EFSA concerning access to documents. EFSA had developed a draft guidance on how to implement a provision of the Regulation of the European Parliament and of the Council concerning the placing of plant protection products on the market, which provided that "scientific peer-reviewed open literature, as determined by [the agency], concerning the side effects on health, the environment, and non-target species. . ., shall be added by the applicant [for authorisation to place a plant protection product on the market]." A working group of the agency submitted the draft guidance to two EFSA bodies, some of whose members were external experts, who were invited to submit comments on the draft guidance. As a result of the comments, the working group incorporated changes into the draft guidance. The guidance, as modified, was submitted for public consultation. EFSA stated that it redacted the names of the experts pursuant to Article 4(1)(b), because disclosure of the experts' names would be a transfer of personal data pursuant to Article 8, and the conditions for such transfer were not satisfied. The names of the experts concerned, together with the opinions expressed by them on the draft guidance, were published on the EFSA website.

The applicant requested access to several documents. EFSA granted partial access, but denied access in response to both the initial and confirmatory application to working versions of the draft guidance and comments of the experts on the draft. In a subsequent decision, EFSA granted the individual comments of the external experts, but redacted the names of the experts, pursuant to Article 4(1)(b) and Regulation 45/2001. It stated that provision of the names would constitute a

transfer of personal data under Article 8 of Regulation 45/2001, and that the conditions for such a transfer were not fulfilled.

Definition of personal data: The information as to which expert is the author of each comment made by the external experts constitutes information which falls within the scope of personal data. The fact that the information is provided as part of a professional activity does not mean that it cannot be characterized as personal data. The concepts of personal data and data relating to private life are not to be confused. The claim that the information concerned does not fall within the scope of private life is therefore ineffective.

Likewise, the fact that both the identity of the experts concerned and the comments submitted on the draft guidance were made public on the EFSA website does not mean such data cannot be characterized as personal data.

Finally, characterization of information relating to a person as personal data does not depend on whether the person objects to the disclosure of that information. (¶¶ 29-33)

Access: Where an application is made seeking access to personal data, the provisions of Regulation 45/2001 (particularly Article 8(b)) become applicable in their entirety. Under Article 8(b), personal data may generally be transferred only if the recipient establishes necessity and if there is no reason to assume that the transfer might prejudice the legitimate interests of the data subject. Thus, the transfer is subject to these two cumulative conditions being satisfied. The applicant must establish the first condition, and the institution must determine whether there is such reason. If there is no such reason, the transfer must be made; if there is such reason, the institution must weigh the various competing interests in order to decide on the request. (¶¶ 44-47)

Necessity/proportionality: No automatic priority can be conferred on the objective of transparency over the right to protection of personal data. However, the information was necessary to ensure the transparency of the process of adoption of a measure likely to have an impact on the activities of economic operators, in particular, to appreciate how the form of participation by each expert might have influenced the content of that measure. Transparency of the process followed by a public authority for adoption of a measure contributes to the authority acquiring greater legitimacy in the eyes of the persons to whom the measure is addressed and increasing their confidence in that authority, and ensuring the authority is more accountable to citizens in a democratic system. Obtaining the information at issue was therefore necessary so that the impartiality of each expert in carrying out their tasks as scientists in the service of EFSA could be ascertained. Thus, the public interest justified the disclosure of the information at issue, in accordance with Article 8(a) and (b). (¶¶ 51-58)

Access to documents: The consideration that disclosure was likely to undermine the privacy and integrity of the experts concerned is a consideration of a general nature not otherwise supported by any factor specific to the case. Disclosure would have made it possible for suspicions of partiality to be dispelled or allowed the experts to dispute the merits of those allegations. If a general consideration, unsupported by evidence, were to be accepted, it could be applied to any situation where an EU authority obtains experts opinions, contrary to the requirement that exceptions to the right of access to documents must be interpreted strictly. Thus, the conditions required by Article 8(b) were satisfied. (¶¶ 69-71)

1.29. C-201/14, SMARANDA BARA ET AL. V. PRESEDINTELE CASEI NATIONALE DE ASIGURARI DE SANATATE (CNAS) ET AL., 1.10.2015 ("BARA")

Reference for a preliminary ruling by the Romanian Court of Appeal. Applicants earn income from self-employment. Data relating to their declared income was transferred by ANAF (the national tax authority) to CNAS (the national health insurance authority); the latter sought payment of arrears of contributions to the health insurance regime, based on this data. The applicants challenged the lawfulness of the transfer of tax data relating to their income, alleging that the data were used for purposes other than those for which they had initially been provided to ANAF, without their prior explicit consent and without having been previously informed.

Questions referred (partial listing): Whether personal data may be processed by authorities for which such data were not intended where such an operation gives rise, retroactively, to financial loss.

Definition of personal data: Tax data transferred are personal data, since they are "information relating to an identified or identifiable natural person." (¶ 29)

Definition of processing: Both the transfer of the data by ANAF, and the subsequent processing by CNAS, constitute processing of personal data. (¶ 29)

Information: The requirement of fair processing laid down in Article 6 of Directive 95/46 requires a public administrative body to inform the data subjects of the transfer of their data to another public administrative body for the purpose of their processing by the latter in its capacity as recipient of those data. National law required the transfer of data necessary to certify that the person concerned qualifies as an insured person to CNAS. However, these do not include data relating to income, since the law recognises the right of persons without a taxable income as qualifying as insured. Thus, the national law cannot constitute "prior information" under Article 10 of Directive 95/46 (information requirement where data collected from the data subject), enabling the controller to dispense with his obligation to inform the data subject of the recipients of the income data, and the transfer therefore violated Article 10. (¶¶ 34-38)

Article 11 (information requirement where data not collected from the data subject) requires that specified information be provided to the data subject, including the categories of data concerned and the existence of the rights of access and rectification. Thus, the data subjects should have been informed of the processing by CNAS and categories of data concerned, but CNAS did not so inform them. The Protocol between the two agencies does not establish rules for derogating from this requirement, either under Article 11 or 13 of the Directive. (¶¶ 42-45)

Derogations: Article 13(1)(e) and (f) provide exceptions for important economic or financial interest of a Member State and monitoring, inspection or regulatory function, respectively. However, Article 13 expressly requires that such restrictions are imposed by legislative measures. Here, however, the transfer was made on the basis of a protocol between the two authorities, which is not a legislative measure, and is not subject to an official publication. Thus, the conditions of Article 13 were not complied with. (¶¶ 39-41)

1.30. C-230/14, WELTIMMO S.R.O. V. NEMZETI ADATVEDELMI ES INFORMACIOSZABADSAG HATOSAG (HUNGARIAN DPA), 1.10.15 ("WELTIMMO")

Reference for a preliminary ruling by the Kuria (Hungary). The applicant, a Slovakian company with no registered office or branch in Hungary (but which carries out no activity where it has its registered office, in Slovakia), runs a website in Hungarian concerning Hungarian properties, with respect to which it processes the personal data of the advertisers. The advertisements are free of charge for one month but thereafter a fee is payable. Many advertisers sent a request by e-mail for deletion of their advertisements and their personal data following the one month period. The applicant did not delete the data and charged the interested parties for its services. These amounts were not paid, so the applicant forwarded the personal data of the advertisers to debt collection agencies. The advertisers lodged a complaint with the Hungarian DPA, which decided that the collection of the data constituted processing, and imposed a fine on the applicant for infringement of the Hungarian data protection law.

Questions referred: (1) Whether Article 28(1) of Directive 95/46 can be interpreted as meaning that the provisions of national law of a Member State are applicable in its territory to a situation where the controller runs a property dealing website established only in another Member State and advertises properties in the territory of the first Member State and the property owners have forwarded their personal data to a facility for storage and data processing belonging to the operator of the website in that other Member State; (2) Whether Article 4(1)(a) (and other provisions) of Directive 95/46 can be interpreted as meaning that the Hungarian DPA may not apply Hungarian data protection law to an operator of a property dealing website established only in another Member State, even though it advertises Hungarian property whose owners transfer the data relating to such property probably from Hungarian territory to a server and processing belonging to the operator of the website; (3) Whether it is significant that the service provided by the controller of the website is directed at the territory of another Member State; (4) Whether it is significant that the data relating to the properties in the other Member State and the personal data of the owners are uploaded from the territory of the other Member State; (5) Whether it is significant that the personal data relating to those properties are that of citizens of another Member State; (6) Whether it is significant that the owners of the undertaking established in Slovakia live in Hungary; (7) Whether the Hungarian DPA can only exercise the powers provided by

Article 28(3) of Directive 95/46 in accordance with the provisions of the national law of the establishment and accordingly not impose a fine.

Definition of processing: The operation of loading personal data on an internet page constitutes processing. (¶ 37)

Establishment of the controller: Article 4(1)(a) of Directive 95/46 permits application of data protection law of a Member State other than the Member State in which the controller is registered, insofar as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity, even minimal, in the context of which the processing is carried out. To establish whether the controller has an establishment in that Member State, both the degree of stability of the arrangements and the effective exercise of activities in the other Member State must be interpreted in light of the specific nature of the economic activities and provision of services concerned, particularly for undertakings offering services exclusively over the internet. The presence of only one representative can suffice to constitute a stable arrangement if he/she acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State. Further, the concept of "establishment" extends to any real and effective activity, even a minimal one, exercised through stable arrangements. (¶¶ 28-31)

Here, the activity of the controller consists in the running of property dealing websites concerning properties in Hungary and written in Hungarian and thus pursues a real and effective activity in Hungary. Further, it has a representative in Hungary responsible for recovering the debts resulting from that activity and representing the controller in administrative and judicial proceedings relating to the processing of the data concerned. It has a bank account in Hungary intended for the recovery of debts and uses a letter box in Hungary for the management of everyday affairs. That is capable of establishing the existence of an "establishment". (¶¶ 32-33)

The processing is done in the context of the activities which Weltimmo pursues in Hungary. Thus Hungarian data protection law would apply with respect to that processing. (By contrast the nationality of the persons concerned by such data processing is irrelevant.) (¶¶ 38-40)

DPA powers: In the event that the Hungarian DPA should consider that Weltimmo has an establishment not in Hungary, but in another Member State, then in accordance with Article 28(4), it may exercise its powers conferred under Article 28(3) only within its own territory, and it may, irrespective of the applicable law and before even knowing which national law is applicable, thereby investigate the complaint. If it becomes apparent that it is the law of another Member State that applies, that DPA cannot impose penalties outside the territory of its own Member State. In fulfillment of the duty of cooperation laid down in Article 28(6), it requests the DPA of that Member State to establish an infringement of its national law and impose penalties if that law permits, based on the information which the first DPA has transmitted to second DPA. The second DPA may also find it necessary to carry out other investigations, on the instructions of the first DPA. (¶¶ 44-58)

1.31. C-362/14, SCHREMS V. DATA PROTECTION COMMISSIONER, 6.10.2015 ("SCHREMS")

Reference for a preliminary ruling by the Irish High Court. The applicant, an Austrian national residing in Austria, was a user of Facebook since 2008, for which he had concluded a contract with Facebook Ireland, a subsidiary of Facebook Inc. located in the USA. Some or all of Facebook Ireland's users data of users who reside in the EU is transferred to the servers in the USA of Facebook Inc. and further processed. The applicant asked the defendant to prohibit Facebook Ireland from transferring his personal data to the USA, which does not ensure adequate protection against the surveillance activities engaged in there by public authorities, in particular the NSA. Defendant rejected the complaint on grounds that there was no evidence that it had been accessed by the NSA and that the Commission decision 2000/520 had found that the USA ensures an adequate level of protection in the Safe Harbor program.

Questions referred: (1) In the course of determining a complaint made to a national DPA that personal data is being transferred to a third country (the USA) the laws and practices of which, it is claimed, do not contain adequate protections for the dt subject, whether that office holder is bound by the EU finding to the contrary in Decision 2000/520, having regard to Articles 7, 8 and 47 CFR, and the provisions of Article 25(6) of Directive 95/46 notwithstanding; (2) Whether the DPA may

and/or must conduct his/her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published.

Independence of DPA: The Directive seeks to ensure an effective, complete, and high level of protection of the fundamental rights and freedoms of natural persons. The guarantee of a DPA's independence is intended to ensure effectiveness and reliability of the monitoring of compliance, and is an essential component of data protection. DPAs powers extend to their own Member State, but not to processing in third countries. However, DPAs are responsible for monitoring transfers from a Member State to a third country, as the transfer is processing carried out in the Member State. (¶¶ 40-47)

An adequacy decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46 is addressed to the Member States, which must take the necessary measures to comply with it. Until the Commission decision is declared invalid by the ECJ, it has legal effect in the Member States. However, it cannot eliminate or reduce the powers of the DPA accorded by Article 8(3) of the CFR, and therefore cannot prevent data subjects whose personal data has been transferred from lodging a claim pursuant to Article 28(4) with the DPA, alleging that an adequate level of protection is not ensured in that third country, which in essence challenges the validity of the Commission's adequacy decision. But the ECJ alone has jurisdiction to declare that the decision is invalid; neither the DPA nor a national court may do so. The latter must refer the claim to the ECJ for a preliminary ruling to examine the validity of the Commission decision. (¶¶ 51-64)

Article 3 of Decision 2000/520 lays down specific rules regarding DPA's powers in light of a Commission adequacy finding (to suspend data flows to self-certified US organisations under restrictive conditions establishing a high threshold for intervention). It excludes the possibility of DPA's taking action to ensure compliance with Article 25 (adequacy), in particular, it denies DPAs powers which they derive from Article 28 to consider a data subject claim which puts into question whether a Commission adequacy decision is compatible with protection of privacy and fundamental rights and freedoms of individuals. This goes beyond the power conferred on the Commission in Article 25(6). Thus, Article 3 is invalid. (¶¶ 100-104)

Adequate level of protection: The word "adequate" in Article 25(6) signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed by the EU legal order. However, it requires the third country to ensure, by reason of its domestic law or international commitments, a level of protection of fundamental rights and freedoms *essentially equivalent* to that guaranteed by the EU by virtue of Directive 95/46 read in light of the CFR, otherwise that protection could be easily circumvented by transfers. Thus, the legal order of the third country covered by a Commission adequacy decision must have means to ensure protection essentially equivalent to that guaranteed within the EU. When examining the level of protection afforded by a third country, the Commission must assess the content of the applicable rules resulting from domestic law or international commitments and the practice designed to ensure compliance. Also, in light of the fact that the level of protection ensured by the third country is liable to change, the Commission must, after adopting an adequacy decision, check periodically whether the adequacy finding remains factually and legally justified. Account must be taken of the circumstances that have arisen after the adoption of the decision. The Commission's discretion as to adequacy is reduced and is subject to strict scrutiny, in view of the important role played by data protection in the light of the fundamental right to respect for private life and the large number of persons potentially concerned by transfers. (¶¶ 73-78)

Safe harbour: US public authorities are not required to comply with safe harbor principles. Decision 2000/520 specifies that safe harbor principles may be limited to the extent necessary to meet national security, public interest or law enforcement requirements, or statute, regulation or caselaw. Self-certified US organisations receiving personal data from the EU are thus bound to disregard safe harbor principles when they conflict with US legal requirements. Decision 2000/520 does not contain sufficient findings regarding US measures which ensure adequacy by reason of domestic law or international commitments. (¶¶ 82-87)

Interference with fundamental right: Decision 2000/520 enables interference with the fundamental right to respect for private life of persons whose personal data is or could be transferred from the EU to the US. (¶87)

Necessity/proportionality: The Decision does not contain any finding regarding US rules intended to limit the interference when they pursue legitimate objectives such as national security,

nor refer to effective legal protection against such interference. FTC procedures and private dispute resolution mechanisms concern compliance with safe harbor principles (against US organisations) and cannot be applied with respect to measures originating from the State. Moreover, the Commission found that US authorities could access the personal data transferred and process it in a way incompatible with the purposes for which it was transferred, and beyond what was strictly necessary and proportionate for the protection of national security, and data subjects had no redress regarding their rights of access, rectification and erasure. Legislation permitting public authorities to have generalized access to the content of electronic communications compromises the essence of the fundamental right to respect for private life. Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access, rectification or erasure of his own personal data does not respect the essence of the fundamental right to effective judicial protection. (¶¶ 88-95)

Thus, Article 1 of the Decision does not ensure adequacy and the decision is consequently invalid. (¶ 98)

Articles 1 and 3 are inseparable from 2 and 4 and the annexes, thus the entire Decision 2000/520 is invalid. (¶105)

2. GENERAL COURT DECISIONS

2.1. T-320/02, ESCH-LEONHARDT AND OTHERS V EUROPEAN CENTRAL BANK, 18.2.2004 ("ESCH-LEONHARDT")

Application for annulment of ECB decision to include in applicants' personal files a letter concerning their use of the internal e-mail system for transmitting union information, and for damages.

Definition of processing: Inclusion of the letters in the personal files constitutes processing by saving data in a personal data filing system as provided in Article 2(a), (b) and (c) of Regulation 45/2001.

Necessity/proportionality: The ECB may be entitled to consider that inclusion of the letters is necessary for the performance of their contracts of employment. Insofar as the letters send a warning to those concerned, they relate to their administrative status and may become relevant for a report on their conduct in the service; thus it is appropriate to include them. A shortened version, omitting reference to relations between those concerned and the trade union, would not be sufficient for proper management of personal files. The fact that the staff in question contravened rules on the use of the ECB's internal email system by using it, as members of trade union, for purposes of that union, and not for gainful purposes, is liable to influence the assessment of their conduct in the service.

Sensitive data: Inclusion of the letters does not infringe Article 10(1) as it concerns data which the persons themselves have manifestly made public within the meaning of Article 10(2)(d).

2.2. T-198/03, BANK AUSTRIA CREDITANSTALT AG V COMMISSION OF THE EUROPEAN COMMUNITIES, 30.5.2006 ("BANK AUSTRIA")

Application for annulment of decision of Commission's hearing officer to publish the non-confidential version of a Commission decision in a cartel case. The applicant (a legal person) argued, inter alia, that in numerous passages of the decision, it was possible to identify natural persons who participated on its behalf in meetings, the purpose of which was to restrict competition, which contravenes Regulation 45/2001.

Legal person: A legal person does not belong to the circle of persons which Regulation 45/2001 is intended to protect. That conclusion cannot be invalidated by the applicant's arguments of its supposed obligations towards directors and employees under Member State law, given that they consist of unsubstantiated contentions. These arguments are not sufficient to demonstrate the applicant's personal interest in relying on a breach of Regulation 45/2001. (¶ 95)

2.3. T-259/03, NIKOLAOU V. COMMISSION, 12.9.2007 ("NIKOLAOU")

Action for non-contractual liability based on acts and omissions of OLAF. OLAF had disclosed certain information about its investigation concerning the applicant: a leak of information to a journalist; its annual report with information about the investigation; and its press statement. The applicant had requested access to the file and the final case report.

Non-contractual liability: Normal rule is that the burden of proof is on the applicant to establish: i) the illegal action of an institution; ii) damages; iii) proof that the damages were caused by the illegal action of the institution. However, the burden of proof shifts to the institution when a fact giving rise to damages could have resulted from various causes, and the institution has not introduced any element of proof as to which was the true cause, even though it was best placed to do so. The Court concluded that the OLAF staff member leaked information (including PD) to a journalist, which was published, and OLAF's press release confirmed the veracity of facts (including PD) that had been mentioned in several press articles. (¶¶ 194-199)

Definition of personal data: The information published in the press release was personal data, since the data subject was easily identifiable, under the circumstances. The fact that the applicant was not named did not protect her anonymity. (¶ 222)

Definition of processing: 1. the leak (unauthorised transmission of personal data to a journalist by someone inside OLAF) and 2. the publication of press release each constitute processing of personal data. (¶ 204)

Lawfulness: The leak constitutes unlawful processing in violation of Article 5 of Regulation 45/2001 because it was not authorized by the data subject, not necessary under the other sub-paragraphs and it did not result from a decision by OLAF. Even though OLAF has a margin of discretion on transmissions, here it was not exercised because the leak is an unauthorized transmission. OLAF is best placed to prove how the leak occurred and that the Director of OLAF did not violate his obligations under Article 8(3) of Regulation 1073/99. In the absence of such proof, OLAF (the Commission) must be held responsible. No concrete showing was made of an internal system of control to prevent leaks or that the information in question had been treated in a manner that would guarantee its confidentiality. (¶¶ 206-209)

Publication of the press release was not lawful under Article 5(a) and (b) because the public did not need to know the information published in the press release at the time of its publication, before the competent authorities had decided whether to undertake judicial, disciplinary or financial follow-up. (¶224)

Damages: A violation of Regulation 45/2001 qualifies as an illegal act of an institution conferring rights on an individual. The objective of the Regulation is to confer such rights on DSs.

- A leak of personal data is necessarily a grave and manifest violation. The Director has a margin of appreciation on prevention, but here no showing was made regarding the exercise of the margin.

- OLAF gravely and manifestly exceeded the limits of its discretion in the application of Article 5(a) and (e), which was sufficient to engage the responsibility of the Community.

- 3000 euros damages were awarded. (¶ 333)

2.4. T-161/04, JORDANA V. COMMISSION, 7.7.2011 ("JORDANA")

Action for annulment of Commission decision refusing the applicant's request under Regulation 1049/2001 for access to the reserve list of successful candidates for a competition, in which he was himself a successful candidate, and for individual decisions nominating officials of grade A6 from 5.10.1995. The Commission had declined his request, based on the exception in Article 4(1)(b) of Regulation 1049/2001 regarding the right of privacy and integrity of the individual. The Commission reasoned that the candidates had not been informed in the notice of competition that the list of laureates would be published, and thus it would violate their private life to provide him with the list. The Commission stated in its reply that it may be possible for the applicant to gain

access on the basis of Regulation 45/2001, and invited the applicant to present a request under that Regulation to the controller. The applicant's confirmatory application was also rejected. (The EDPS intervened in the case).

Article 4(1)(b): This provision is indivisible, and requires that the violation of private life and the integrity of the individual are always analyzed in conformity with the right to protection of personal data. Thus it establishes a specific regime where personal data may be communicated to the public. Since this case concerns the processing of personal data, the request must be analyzed under Regulation 45/2001. In rejecting the application for access to documents, the Commission had failed to apply Regulation 45/2001 in its analysis, and thus erred. (¶¶ 99-100)

Definition of personal data: The first and last names of the persons on the reserve list and the officials mentioned in the individual decisions of appointment to grade A6 can be considered to fall within the personal data definition. (¶ 91)

Definition of processing: Transfer of the data constitutes processing. (¶ 91)

2.5. T-82/09, DENNEKAMP V. EUROPEAN PARLIAMENT, 23.11.2011 ("DENNEKAMP I")

Application for annulment of European Parliament decision refusing to grant access to documents under Regulation 1049/2001 relating to the affiliation of certain MEPs to the additional pension scheme. Parliament had refused access on the ground that disclosure would be incompatible with Regulation 45/2001. At the hearing, the applicant submitted that he needed to have access to the personal data on grounds of public interest in accountability, transparency and control over public expenditure.

Balancing fundamental rights: Regulation 1049/2001 and Regulation 45/2001 do not contain any provisions granting one primacy over the other, therefore full application of both should, in principle, be ensured. (¶ 24)

Article 8(b): Where a request based on Regulation 1049/2001 seeks access to documents containing personal data, Regulation 45/2001 becomes applicable in its entirety, including Article 8. The applicant cannot claim that the processing he requested was lawful on the basis of Article 5(b) and this suffices, since Article 8(b) applies without prejudice to Article 5. (¶¶ 26-29)

In order to obtain disclosure of the personal data contained in the documents, the applicant would have had to demonstrate, by providing express and legitimate justifications, the necessity for the requested personal data to be transferred, so that the Parliament could weigh up the various interests of the parties concerned and determine whether legitimate interests of MEPs might be prejudiced by the transfer. The applicant failed to establish why he needed the names to obtain his objectives. He did not explain with express arguments and justifications in what respect the transfer of the data was necessary to satisfy the public interest which he invoked, nor that the transfer would have been proportionate to his aims. (¶¶ 26-29)

Further, the Parliament was not required to weigh the interests invoked by the applicant against those of MEPs, or to determine whether there was any reason to assume that the legitimate interests of those MEPs might have been prejudiced by such transfer. Thus, no manifest error that the Parliament might have made in weighing up interests has any bearing in this case on the lawfulness of the decision. (¶ 44)

Article 4(1)(b): This is an indivisible provision requiring the institution concerned always to examine and assess any undermining of privacy and the integrity of the individual in conformity with Regulation 45/2001. (¶ 39)

2.6. T-190/10, EGAN & HACKETT V. EUROPEAN PARLAMENT, 28.3.2012 ("EGAN & HACKETT")

Application for annulment of European Parliament decision denying access to certain documents. The applicants, who had worked for former MEPs, requested access to certain documents, which they stated they needed to commence legal proceedings. Among the documents requested were lists of assistants open for public inspection since 1984. Access was denied to the

list on grounds of Article 4(1)(b) of Regulation 1049/2001 and Regulation 45/2001, except that lists open to the public during the period of professional activity of the persons.

Scope of Regulation 45/2001: Neither Article 2(3) of Regulation 1049/2001, nor Article 3(2) of Regulation 45/2001, nor any other provision, contains any restriction such as to exclude from their respective scopes documents which were, but are no longer, available. (¶ 74)

Access: The Parliament systematically took the view that the public should not have access to documents revealing the identity of former MEP assistants. It did not carry out an examination to show that the access would specifically and effectively undermine their privacy within the meaning of the provisions in question, nor did it verify whether the risk of the protected interest being undermined was reasonably foreseeable and not purely hypothetical. Thus, it failed to show to what extent disclosure would specifically and effectively undermine the right to privacy. (¶¶ 89-94)

Sensitive data: The argument that release of names of former MEP assistants would reveal their political opinions and therefore constitute sensitive data was not substantiated and cannot make up for the fact that the contested decision failed to show why disclosure would specifically and effectively undermine their right to privacy within the meaning of Article 4(1)(b) of Regulation 45/2001. (¶ 101)

2.7. T-115/13, DENNEKAMP V. EUROPEAN PARLIAMENT (15.7.2015) ("DENNEKAMP II")

Application for annulment of European Parliament decision refusing to grant access to documents under Regulation 1049/2001 relating to the affiliation of certain MEPs to the additional pension scheme. This case is related to case T-82/09, Dennekamp v. European Parliament, 23.11.2011. After receiving the judgment in that case, the applicant submitted a new request for access to four categories of documents relating to affiliation of certain MEPs to the additional pension scheme. He stated in the application that there was an objective necessity for the personal data to be transferred, relying on a broad public interest in transparency and how decisions were taken; that it was of the utmost importance for European citizens to know which MEPs had a personal interest in the additional pension scheme which involved the use of considerable public funds; and in the confirmatory application, he relied on the rights to information and freedom of expression. The EP denied access to three of the four categories, and confirmed the decision in response to the applicant's confirmatory application. The applicant sought annulment of the EP's decision.

Transfers: Articles 7-9 of Regulation 45/2001 precisely limit the possibility of transferring personal data so as to make it subject to strict conditions which, if not fulfilled, prohibit any transfer. Those conditions always include the necessity of the transfer in the light of various aims. (¶ 58)

Balancing fundamental rights: If the applicant has established necessity, and the institution decides there is no reason to assume that DS' legitimate interests may be prejudiced, the data may be transferred and the documents are to be made available to the public. To fulfill the condition of necessity under that article, an applicant for access to documents containing personal data must establish that the transfer of personal data is the most appropriate of the possible measures for attaining the applicant's objective, and it is proportionate to that objective, which means the applicant must submit express and legitimate reasons to that effect. This strict interpretation cannot be regarded as creating a broad exception to the fundamental right of access to documents which would result in an unlawful restriction of that right. Rather, it reconciles two fundamental yet opposing rights, the institution being required also to examine whether the legitimate interests of the data subjects might be prejudiced by the transfer. The general nature of the justification for transfer has no direct effect on whether the transfer is necessary for the purposes of attaining the applicant's aim. (¶¶ 60-61)

Here the applicant made two arguments to establish necessity. First, that necessity was based on the right to information and freedom of expression. These are not sufficient to establish that the transfer is the most appropriate of the possible measures for attaining the objective, or that it is proportionate to that objective. Moreover, the applicant did not make clear in what respect transferring the names of the MEPs participating in the scheme was the most appropriate measure for attaining the objective he had set for himself. He merely asserted that the measures designed to provide public control over public expenditure in the context of the additional pension scheme,

like the discharge procedure, did not protect the fundamental right to information and to communicate it to the public. From this it cannot be determined in what respect the transfer would be the most appropriate measure, or how it is proportionate. (¶¶ 81-87)

Second, the applicant argued that the transfer of personal data is necessary to determine whether MEPs' voting behavior regarding the additional pension scheme is influenced by their financial interest, and disclosure of all the names of the MEPs participating in the scheme would be the only way for the public to hold its representatives accountable for their actions in relation to the scheme. The court agreed that the transfer is the only measure by which the applicant's aim can be attained; no other measure is capable of ensuring that MEPs facing a potential conflict of interest are identified. Further, it is proportionate for this purpose. (¶¶ 88-94)

The EU institution or body in receipt of the application must refuse the transfer if there is the slightest reason to assume that the data subjects' legitimate interests would be prejudiced. MEPs as public figures have chosen to expose themselves to scrutiny by third parties, particularly the media and general public, even if such choice in no way implies that their legitimate interests must be regarded as never being prejudiced by a decision to transfer their data. Thus, they have generally already accepted that some of their personal data will be disclosed to the public. That must be taken into account when assessing the risk of prejudice to their legitimate interests. Particular consideration should be given to the link between the personal data at issue and their mandate, and to the legal and financial commitment of the EP to the scheme. In view of the importance of the interests invoked here, which are intended to ensure the proper functioning of the EU by increasing the confidence that citizens may legitimately place in the institutions, the legitimate interests of the MEPs who are members of the scheme cannot be prejudiced by the transfer of personal data at issue. (¶¶ 115-131)

An institution which refuses access on the ground of prejudice to legitimate interests must state reasons for invoking such interests. The institution must explain how disclosure of a document could specifically and actually undermine the interest protected by the exception. The explanation cannot consist of a mere assertion that access would undermine privacy. Examination of the specific and actual nature of the undermining of the interest under Article 4(1)(b) of Regulation 1049/2001 is indissociable from the assessment of the risk that the legitimate interests of the data subject referred to in Article 8(b) of Regulation 45/2001 which, through the disclosure to the public, might be prejudiced by the transfer of personal data. (¶¶ 133-135)

2.8. T-496/13, McCULLOUGH V. CEDEFOP (11.6.2015)("McCULLOUGH")

Application for annulment of Cedefop's decision refusing access to documents. The applicant, who had been employed by Cedefop, requested access to the minutes of all meetings of various internal groups for a specified period stating that he needed them to prepare his defence in legal proceedings between him and Cedefop pending before the Greek courts. Access was denied on the basis of Article 4(1)(b) and 4(3), and on grounds that Cedefop was not in possession of some of the requested documents, in response the initial and confirmatory applications. Regarding minutes of the Governing Board and its Bureau, Cedefop considered that the names of the members which were contained in those minutes constituted personal data protected by Regulation 45/2001, and access could lead to a serious violation of the privacy and integrity of the members, as their opinions would be clearly shown in the documents. The applicant argued that the names and functions of the members of Cedefop's Governing Board and Bureau are not personal data and that Cedefop's statement that disclosure of the members opinions and views would violate their privacy is contrary to the principle of transparency (among others).

Definition of personal data: Surnames are personal data and therefore are protected by Regulation 45/2001. The fact that the members of Cedefop's decision-making bodies participated in the meetings of those bodies in connection with the exercise of their public duties and not in the private sphere, and that the surnames were published in the OJ or on the internet, does not affect the characterization of the surnames as personal data. (¶ 66)

Transfer: Applicant cannot be deemed to have proved the necessity of having the personal data at issue transferred. The only justification provided was to supplement his written defence before the Greek Examining Magistrate. Applicant did not provide any information or justification as to how the submission of the requested documents containing that data would affect the Greek proceedings, the risks to which he would be exposed in procedural terms, and the merits of his defence if the documents were not submitted to the Greek Magistrate. (¶¶ 69-70)

Article 4(1)(b): Exceptions under Article 4 must be interpreted and applied strictly. An institution refusing access must explain how disclosure of that document could specifically and actually undermine the interest protected by the exception. Fact that a document concerns an interest protected by an exception is not of itself sufficient to justify application of that exception. Rather, it is necessary for institution to have previously determined (1) that the document would specifically and actually undermine the protected interest and (2) that the risk of the protected interest being undermined is reasonably foreseeable and not purely hypothetical. Institution must explain how granting access to the document could specifically and actually undermine the interest protected by the exception under Article 4(1)(b).

Here, Cedefop simply states that the persons concerned are protected as individuals and any access would lead to a serious violation of the privacy and integrity of the individual as they clearly demonstrated the opinions and views of the members on the subject matters discussed. However, Cedefop neither carried out an examination demonstrating that granting access to those documents would specifically and actually undermine the privacy of those members within the meaning of Article 4(1)(b), nor verified whether the risk of the protected interest being undermined was reasonably foreseeable and not purely hypothetical. It is not apparent how the opinions and views expressed could fall within the sphere of their privacy, since those meetings were professional. (¶¶ 82-88)

3. CIVIL SERVICE TRIBUNAL DECISIONS

3.1. F-30/08, NANOPOULOS V. COMMISSION, 11.5.2010 ("NANOPOULOS") (ON APPEAL, CASE T-308/10)

Action for non-contractual liability against the Commission pursuant to Article 340 TFEU. A journalist sent a letter to the Commission asking about anonymous allegations that the applicant favored companies of his own nationality in performing his duties as a Director in the Commission. The Commission reassigned the applicant to a post of principal advisor to the Director General, and opened a disciplinary proceeding against the applicant. Two leaks occurred: one concerning the plan to reassign the applicant; and one concerning the Commission's decision to open a disciplinary proceeding against the applicant. Journal Articles thereafter were published with the applicant's name including these facts.

Non-contractual liability: The normal rule is that the burden of proof is on the applicant to establish: i) the illegal action of an institution; ii) damages; iii) proof that the damages were caused by the illegal action of the institution. However, the burden of proof shifts to the institution when a fact giving rise to damages could have resulted from various causes, and the institution has not introduced any element of proof as to which was the true cause, even though it was best placed to do so. The publication of the applicant's name could only have resulted from a leak by the Commission. The burden of proof was on the Commission to prove that it was not the source of the leak. (¶161)

Damages: The leak by the Commission of the complainant's name as one of the officials undergoing a disciplinary procedure constitutes a violation of Regulation 45/2001, which was sufficient to engage its responsibility. 90.000 euros damages were awarded (70.000 moral prejudice and 20.000 fault of service linked to moral prejudice). (¶¶ 244-250)

3.2. F-46/09, V & EDPS V. EUROPEAN PARLAMENT, 5.7.2011 ("V")

Application for annulment of a decision of the European Parliament, withdrawing a 2008 offer of employment to the applicant on grounds of unfitness to be hired. The Commission Medical Service had determined that the applicant was not fit; she had appealed, and the Commission had affirmed the conclusion. She filed an Article 90 complaint, which the Commission rejected, then a lawsuit against that decision, which the Court of First Instance rejected. In 2008, she was offered a post as contractual agent with the Parliament. The Parliament requested and received a copy of her medical file from the Commission medical service and thereafter withdrew its offer on the ground that she was unfit to work in any of the EU institutions. The applicant filed an Article 90 complaint against this decision, which the Parliament rejected. In the action before the court, the applicant alleged that her medical dossier collected by the Commission should have been used only with respect to her recruitment by the Commission. Further, the medical counsel of the Parliament should have only examined her and not inquired on her past medical history.

(The EDPS brief stated that the transfer violated Regulation 45/2001. First, the data are not part of the applicant's medical dossier as former temporary agent and former contractual agent of the Commission. The procedural manual of the Commission's medical service does not indicate the ends for which medical data collected during a recruitment procedure are saved in the archive for more than 6 months, nor the conditions under which they are accessible. In opinions to the Parliament and Commission, he recommended that for candidates deemed unfit for hiring, the medical data collected during the recruitment procedure should only be held for a limited period, corresponding to the period during which it is possible to contest the data or the decision taken on the basis of the data. Further, the transfer is governed by Article 7, without prejudice to Articles 4, 5, 6 and 10. Respect of Article 7 thus does not render the transfer and ultimate use of the data legal under the Regulation in its totality. By virtue of Article 10, paragraph 1, the processing of special categories of data is prohibited and the protection of such data has, for the ECHR, a fundamental importance for exercise of the right to privacy, guaranteed by Article 8 of the Convention. The applicant did not give her consent to the transfer, in accordance with the exception foreseen in Article 10, paragraph 2. Further, the Parliament did not show that the transfer was really necessary to respect the statute, within the meaning of the Article 10(2)(b). It would have been possible to obtain the information in a less intrusive manner. Once received by the Parliament, the data were no longer being used for the purpose for which they were collected. The transfer and use of the data violated Article 4(1)(b) and (e).)

Article 8 ECHR: This is a fundamental right which covers the right to secrecy of one's medical state. The transfer of that data to a third party, even another EU institution, is an interference with that right, whatever the final use. Such interference may be justified if it is "in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." (¶¶ 113, 123)

- In accordance with the law: Regulation 45/2001 establishes that inter-institutional transfers are foreseen. However, Article 7 is very general. Further, Article 6 states that personal data shall only be processed for purposes other than those for which they were collected if the change of purpose has been expressly foreseen by the rules of the EU institution, which was not the case here. (¶¶ 115-119)

- Necessary in a democratic society: This criterion is met if it is necessary to respond to a social imperative, and if proportionate to the legitimate end and the reasons specified are relevant and sufficient. The national authority has a limited margin of discretion. The right to privacy of medical data is protected by EU juridical order, not only to protect the private life of the sick but also to preserve their confidence in the medical body and the medical services in general. The possibility to transfer such data to another institution calls for a particularly rigorous examination. Thus the interest of the Parliament to recruit a person able to exercise his duties must be balanced against the gravity of the interference of the right of the person concerned. The interest of the Parliament to conduct the medical examination does not justify the transfer without the consent of the person concerned. The data are very sensitive, were collected nearly two years before, for a specified purpose, by an institution for which the applicant did not work. The need of the Parliament could have been met by less intrusive means. (¶¶ 122-127)

- Article 6 and 7: Article 1 specifies that EU institutions protect the fundamental rights of natural persons, in particular their right to privacy with respect to processing their personal data. Thus, the provisions of the Regulation may not be read as legitimising an interference to the right to privacy. The purpose for the Commission's collection of the data was to determine the applicant's fitness to perform the duties in the Commission's post. Using them to determine her fitness for the post with the Parliament constituted a change of purpose. Each institution is an independent employer, and is autonomous in the management of its personnel. The change of purpose was not foreseen in any legal text. (¶¶ 128-136)

Sensitive data: The applicant did not consent to the transfer of her data. The transfer was not "necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law," in accordance with Article 10(2)(b). The Parliament's obligation to control fitness for duty could have been achieved by less intrusive means. Nor does Article 10(3) justify the transfer. (¶¶ 137-139)

Damages: 5000 euros material damages, 20.000 moral prejudice. (¶¶ 166, 175-176)

II. SUMMARY OF EU COURT DECISIONS RELATING TO DATA PROTECTION (ORGANISED BY TOPIC)

1. GENERAL

1.1. DEFINITION OF PERSONAL DATA

Lindquist: The name of a person in conjunction with his/her telephone number, and information about his/her working conditions or hobbies constitute personal data. (¶ 24)

Tietosuojavaltuutettu: The surname and given name of certain natural persons whose income exceeds certain thresholds, as well as the amount of their earned and unearned income, constitute personal data. (¶ 35)

Bavarian Lager: Surnames and forenames may be regarded as personal data. Thus the list of names of participants in a meeting is personal data, since persons can be identified. (¶ 68)

Scarlet: ISP addresses are protected personal data because they allow the related users to be precisely identified. (¶ 51)

M: The data relating to the applicant for a residence permit included in the minute (applicant's name, DOB, nationality, gender, ethnicity, religion and language) constitute personal data. The legal analysis in the minute may contain personal data but it does not in itself constitute such data. The legal analysis is not information relating to the applicant, but at most, in so far as not limited to a purely abstract interpretation of the law, is information about the assessment and application by the competent authority of that law to the applicant's situation. This interpretation is consistent with the language of Article 2(a) and the objective and general scheme of Directive 95/46. (¶¶ 34, 38-41)

Schwartz: Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows them to be identified with precision. (¶ 27)

Worten: Data contained in the record of working time concerning, in relation to each worker, the daily work periods and rest periods, constitute personal data because they represent "information relating to an identified or identifiable natural person." (¶ 19)

Englebert: Data collected by private detectives relating to persons acting as estate agents concern identified or identifiable natural persons, and therefore constitute personal data. (¶ 26)

Rynes: The image of a person recorded by a camera constitutes personal data because it makes it possible to identify the person concerned. (¶ 22)

Client Earth: The information as to which expert is the author of each comment made by the external experts constitutes information which falls within the scope of personal data. The fact that the information is provided as part of a professional activity does not mean that it cannot be characterized as personal data. The concepts of personal data and data relating to private life are not to be confused. The claim that the information concerned does not fall within the scope of private life is therefore ineffective.

Likewise, the fact that both the identity of the experts concerned and the comments submitted on the draft guidance were made public on the EFSA website does not mean such data cannot be characterized as personal data.

Finally, characterization of information relating to a person as personal data does not depend on whether the person objects to the disclosure of that information. (¶¶ 29-33)

Bara: Tax data transferred are personal data, since they are "information relating to an identified or identifiable natural person." (¶ 29)

Nikolaou: The information published in the press release was personal data, since the data subject was easily identifiable, under the circumstances. The fact that the applicant was not named did not protect her anonymity. (¶ 222)

Jordana: The first and last names of the persons on the reserve list and the officials mentioned in the individual decisions of appointment to grade A6 can be considered to fall within the personal data definition. (¶ 91)

McCullough: Surnames are personal data and therefore are protected by Regulation 45/2001. The fact that the members of Cedefop's decision-making bodies participated in the meetings of those bodies in connection with the exercise of their public duties and not in the private sphere, and that the surnames were published in the OJ or on the internet, does not affect the characterization of the surnames as personal data. (¶ 66)

1.2. DEFINITION OF PROCESSING

Lindquist: The operation of loading personal data on an internet page must be considered to be processing. (¶ 25)

Tietosuojavaltuutettu: The collection, publication, transfer on a CD-ROM and by text messaging all constitute processing of personal data. This includes personal data that have already been published in unaltered form in the media, as ooperations referred to in Article 2(b) must be classified as processing also where they exclusively concern material that has already been published in unaltered form in the media. A general derogation from the application of the Directive in such a case would largely deprive the Directive of its effect. (¶¶ 35-37)

Bavarian Lager: Communication of personal data in response to a request for access to documents constitutes processing. (¶69)

Bonnier: Communication of name and address sought by applicants constitutes processing of personal data. (¶ 52)

Google: The operation of loading personal data on an internet page must be considered processing (Lindquist). In exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine "collects" such data which it subsequently "retrieves", "records" and "organizes" within the framework of its indexing programmes, "stores" on its servers and, as the case may be, "discloses" and "makes available" to its users in the form of lists of search results, which constitute processing, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data. This finding is not affected by the fact that those data have already been published on the internet and are not altered by the search engine. It is not necessary that the personal data be altered. While alteration of personal data constitutes processing under Article 2(b), the other operations mentioned there do not require the alteration of personal data.

The processing done by the search engine operator is distinguished from and in addition to that done by publishers of websites, consisting in loading those data on an internet page. (¶¶ 26-31)

Schwartz: Taking and storing fingerprints constitute processing. (¶¶ 28-29)

Bara: Both the transfer of the data by ANAF, and the subsequent processing by CNAS, constitute processing of personal data. (¶ 29)

Weltimmo: The operation of loading personal data on an internet page constitutes processing. (¶ 37)

Esch-Leonhardt: Inclusion of the letters in the personal files constitutes processing by saving data in a personal data filing system as provided in Article 2(a), (b) and (c) of Regulation 45/2001.

Nikolaou: 1. the leak (unauthorised transmission of personal data to a journalist by someone inside OLAF) and 2. the publication of a press release each constitute processing of personal data. (¶ 204)

Jordana: Transfer of the data constitutes processing. (¶ 91)

1.3. DEFINITION OF CONTROLLER

Google: The search engine operator determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of the activity and is thus a controller. It would be contrary not only to the clear wording of Article 2(d) and to its objective, which is to ensure through a broad definition of the concept of controller, effective and complete protection of data subjects, to exclude the operator of a search engine on the ground that it does not exercise control over the personal data published on the web pages of third parties. Moreover, the activity of search engines plays a decisive role in the overall dissemination of the personal data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published. The search results also provide a structured overview of the information relating to that individual that can be found on the internet, enabling them to establish a detailed profile of the data subject. The fact that publishers of websites have the option of indicating to operators by means of exclusion protocols that they wish some information published on their site to be excluded from search engines' automatic indexing does not mean if publishers do not so indicate, the operator of the search engine is released from responsibility for its processing of personal data. (¶¶ 33-41)

Rynes: Arts. 7(f), 11(2) and 13(1)(d) and (g) make it possible to take into account the legitimate interests of the controller in protecting the property, health and life of his family and himself. (¶ 34)

1.4. LEGAL PERSONS

Schecke: Legal persons can claim protection of Articles 7 and 8 of the CFR only insofar as the official title of a legal person identifies one or more natural persons. Here, the name of the legal person directly identifies natural persons who are its partners. (¶ 53)

Bank Austria: A legal person does not belong to the circle of persons which Regulation 45/2001 is intended to protect. That conclusion cannot be invalidated by the applicant's arguments of its supposed obligations towards directors and employees under Member State law, given that they consist of unsubstantiated contentions. These arguments are not sufficient to demonstrate the applicant's personal interest in relying on a breach of Regulation 45/2001. (¶ 95)

1.5. SENSITIVE PERSONAL DATA

Lindquist: Reference to the fact that an individual has injured her foot and is on medical leave constitutes personal data concerning health within the meaning of Article 8(1), as that provision must be given a wide interpretation so as to include all aspects, both physical and mental, of the health of an individual. (¶¶ 50-51)

Esch-Leonhardt: Inclusion of a letter concerning an ECB staff member's use of internal e-mail to transmit union information in his personal file does not infringe Article 10(1) as it concerns data which the person himself has manifestly made public within the meaning of Article 10(2)(d).

Egan & Hackett: The argument that release of names of former MEP assistants would reveal their political opinions and therefore constitute sensitive data was not substantiated and cannot make up for the fact that the contested decision failed to show why disclosure would specifically and effectively undermine their right to privacy within the meaning of Article 4(1)(b) of Regulation 45/2001. (¶ 101)

V: The applicant did not consent to the transfer of her medical file by the Commission to the European Parliament. The transfer was not "necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law," in accordance with Article 10(2)(b). The Parliament's obligation to control fitness for duty could have been achieved by less intrusive means. Nor does Article 10(3) justify the transfer. (¶¶ 137-139)

1.6. CONSENT

Schecke: The legislation at issue (EU rules on financing under CAP and publication on internet) does not seek to base the personal data processing for which it provides on consent of the beneficiaries concerned. Rather, it provides that they are to be informed. Thus, processing is not based on their consent. Therefore, it is necessary to analyse whether interference is justified under CFR Article 52(1). (¶ 54)

Schwartz: It is essential for citizens of the EU to own a passport in order to travel to a third country, and a passport must contain fingerprints. Therefore, citizens are not free to object to processing of their fingerprints, and thus persons applying for passports cannot be deemed to have consented to that processing. (¶ 32)

1.7. NECESSITY/PROPORTIONALITY

Huber: Directive 95/46 is intended to ensure an equivalent level of data protection in all Member States, to ensure a high level of protection in the EU. The concept of necessity in Article 7(e) cannot have a meaning which varies among Member States. Thus, it is a concept which has its own independent meaning in EU law, and must be interpreted in a manner which fully reflects the objective of Directive 95/46. (¶¶ 50-52)

Under EU law, the right of free movement of a Member State national is not unconditional, but may be subject to limitations and conditions imposed by the Treaty and implementing rules. Legislation provides that a Member State may require certain documents to be provided to determine the conditions of entitlement to the right of residence. Thus, it is necessary for a Member State to have relevant particulars and documents available to it in order to ascertain whether a right of residence in its territory exists. Use of a register to support authorities responsible for the application of the legislation on the right of residence is, in principle, legitimate. However, the register must not contain any information other than what is necessary for that purpose, and must be kept up to date. Access must be restricted to the responsible authorities. The central register could be necessary if it contributes to a more effective application of that legislation. The national court should decide whether these conditions are satisfied. Only anonymous information is required for statistical purposes. (¶¶ 54-62)

Scarlet: The contested filtering system (to detect e-communications which use file sharing software, with a view to preventing copyright infringement) may infringe the right to protection of personal data of the ISP's customers, as it would involve a systematic analysis of all content and the collection and identification of users' IP address from which unlawful content on the network is sent. (¶¶ 50-51)

Schwartz: Storage of fingerprints on a highly secure storage medium is likely to reduce risk of passports being falsified and to facilitate the work of the authorities responsible for checking the authenticity of passports at EU borders, although it is not wholly reliable. Thus, it is appropriate. (¶¶ 41-45)

The action involves taking prints of two fingers, causing no physical or mental discomfort, plus a facial image. The only real alternative to fingerprints is iris scan, the technology of which is not yet as advanced as fingerprint recognition. Thus, no apparent alternative exists that is sufficiently effective and less of a threat to the protected rights. (¶¶ 48-53)

Concern that data may be centrally stored and used for other purposes (e.g. criminal investigation or to monitor the person indirectly) does not affect the validity of the Regulation, which provides only for preventing illegal entry into the EU. (¶¶ 61-62)

Worten: The referring court must verify that the personal data contained in the record of working time are collected in order to ensure compliance with the national legislation relating to working conditions and that the processing of those data is necessary for compliance with a legal obligation to which Worten is subject and the performance of the monitoring task entrusted to the national authority responsible for monitoring working conditions. Only the grant of access to authorities having powers of monitoring could be considered to be necessary within the meaning of Article 7(e). Further, the obligation to provide immediate access to the record could be necessary if it

contributes to the more effective application of the legislation relating to working conditions. It is for the referring court to decide whether this requirement is necessary. (¶¶ 35-43)

Penalties must respect the principle of proportionality. (¶ 44)

Client Earth: No automatic priority can be conferred on the objective of transparency over the right to protection of personal data. However, the information was necessary to ensure the transparency of the process of adoption of a measure likely to have an impact on the activities of economic operators, in particular, to appreciate how the form of participation by each expert might have influenced the content of that measure. Transparency of the process followed by a public authority for adoption of a measure contributes to the authority acquiring greater legitimacy in the eyes of the persons to whom the measure is addressed and increasing their confidence in that authority, and ensuring the authority is more accountable to citizens in a democratic system. Obtaining the information at issue was therefore necessary so that the impartiality of each expert in carrying out their tasks as scientists in the service of EFSA could be ascertained. Thus, a public interest justified the disclosure of the information at issue, in accordance with Article 8(a) and (b). (¶¶ 51-58)

Esch-Leonhardt: The ECB may be entitled to consider that inclusion of letters concerning ECB staff members' use of internal e-mail to transmit union information in their personal file is necessary for the performance of their contract of employment. Insofar as the letters send a warning to those concerned, they relate to their administrative status and may become relevant for a report on their conduct in the service; thus it is appropriate to include them. A shortened version, omitting reference to relations between those concerned and the trade union, would not be sufficient for proper management of personal files. The fact that the staff in question contravened rules on the use of the ECB's internal email system by using it, as members of a trade union, for purposes of that union, and not for gainful purposes, is liable to influence the assessment of their conduct in the service.

1.8. SECURITY

Worten: Article 17(1) requires controllers (not Member States) to adopt technical and organizational measures which, having regard to the state of the art and cost of their implementation, are to ensure a level of security appropriate to the risks represented. The obligation under national law to provide the national authority responsible for monitoring working conditions with immediate access to the record of working time does not imply that the data must be made accessible to persons not authorised for that purpose (as Worten claimed). Rather, Worten must ensure that only those persons duly authorised to access the personal data in question are entitled to respond to a request for access from a third party. Thus, Article 17(1) is not relevant here. (¶¶ 24-25, 28-29)

1.9. DEROGATIONS

Englebert: The activity of a body such as IPI (a professional body responsible for ensuring compliance with the rules governing the profession of estate agent which is a regulated profession in Belgium, through investigating and reporting breaches of those rules) corresponds to "the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions" and is capable of coming under that exception. The directive does not prevent such a professional body from having recourse to private investigators. Thus, if a Member State has chosen to implement the exception, then the professional body and private detectives may rely on it and are not subject to the obligation to inform the data subject. However, if the Member State has not implemented the exception, the data subjects must be informed. (¶¶ 42-46)

Rules on access to a regulated profession form part of the rules of professional ethics, therefore investigations concerning the acts of persons who breach those rules by passing themselves off as estate agents are covered by the exception in Article 13(1)(d). (¶ 50)

Bara: Article 13(1)(e) and (f) provide exceptions for important economic or financial interest of a Member State and monitoring, inspection or regulatory function, respectively. However, Article 13 expressly requires that such restrictions are imposed by legislative measures. Here, however, the transfer from the Member State tax authority to the health insurance authority on the data subject's declared income was made on the basis of a protocol between the two authorities, which is not a legislative measure, and is not subject to an official publication. Thus, the conditions of Article 13 were not complied with. (¶¶ 39-41)

1.10. NON-CONTRACTUAL LIABILITY

Nikolaou: The normal rule is that the burden of proof is on the applicant to establish: i) the illegal action of an institution; ii) damages; iii) proof that the damages were caused by the illegal action of the institution. However, the burden of proof shifts to the institution when a fact giving rise to damages could have resulted from various causes, and the institution has not introduced any element of proof as to which was the true cause, even though it was best placed to do so. The Court concluded that the OLAF staff member leaked information (including PD) to a journalist, which were published, and OLAF's press release confirmed the veracity of facts (including PD) that had been mentioned in several press articles. (¶¶ 194-199)

A violation of Regulation 45/2001 qualifies as an illegal act of an institution conferring rights on an individual. The objective of the Regulation is to confer such rights on data subjects.

A leak of personal data is necessarily a grave and manifest violation. The Director has a margin of appreciation on prevention, but here no showing was made regarding the exercise of the margin.

OLAF gravely and manifestly exceeded the limits of its discretion in the application of Article 5(a) and (e), which was sufficient to engage the responsibility of the Community.

3000 euros damages were awarded. (¶ 333)

V: 5000 euros material damages, 20.000 moral prejudice, were awarded. (¶¶ 166, 175-176)

2. DATA SUBJECT RIGHTS

2.1. INFORMATION

Bara: The requirement of fair processing laid down in Article 6 of Directive 95/46 requires a public administrative body to inform the data subjects of the transfer of their data to another public administrative body for the purpose of their processing by the latter in its capacity as recipient of those data. National law required the transfer of data necessary to certify that the person concerned qualifies as an insured person to CNAS. However, these do not include data relating to income, since the law recognises the right of persons without a taxable income as qualifying as insured. Thus, the national law cannot constitute "prior information" under Article 10 of Directive 95/46 (information requirement where data is collected from the data subject), enabling the controller to dispense with his obligation to inform the data subject of the recipients of the income data, and the transfer therefore violated Article 10. (¶¶ 34-38)

Article 11 (information requirement where data is not collected from data subject) requires that specified information be provided to the data subject, including the categories of data concerned and the existence of the rights of access and rectification. Thus, the data subjects should have been informed of the processing by CNAS and of the categories of data concerned, but CNAS did not so inform them. The Protocol between the two agencies does not establish grounds for derogating from this requirement, either under Article 11 or 13 of the Directive (¶¶ 42-45).

2.2. ACCESS

Rijkeboer: The right of access is necessary to enable the data subject to exercise his other rights (rectification, blocking, erasure, and notify recipients of same; object to processing or request damages). The right must of necessity relate to the past, otherwise the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for damages. Member States have some freedom of action in implementing the Directive, but it is not unlimited. Setting of a time limit on the right of access must allow the data subject to exercise his rights. It is for the Member States to fix a time limit for storage of information on the recipients and the content of the data disclosed, and to provide access to that information which constitutes a fair balance between the interest of the data subject in exercising his rights and the burden on the controller to store that information. In the present case, limiting storage of information on recipients and content to one year, while the basic data is stored much longer, does not constitute a fair balance, unless it can be shown that longer storage would constitute an excessive burden. (¶¶51-57, 64-66)

M: Regarding the right of access, protection of the fundamental right to respect for private life means that the person may be certain that the personal data concerning him are correct and that they are processed lawfully. It is in order to carry out the necessary checks that the data subject has, under Article 12(a), a right of access, which is necessary to obtain rectification, erasure or blocking of his data (Article 12(b)). The legal analysis is not in itself liable to be the subject of a check of its accuracy by the applicant and rectification, while the facts are. Moreover, the right of access is not designed to ensure the greatest possible transparency of the decision-making process of public authorities and to promote good administrative practices (as is the case for the right of access to documents). (¶¶ 44-46)

To comply with the right of access under Article 12(a) and Article 8(2) of CFR, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with the Directive. He need not be given a copy of the documents. (¶¶ 59-60)

X: Article 12(a) of Directive 95/46 does not require Member States to levy fees when the right of access to personal data is exercised, nor does it prohibit the levying of such fees as long as they are not excessive. Access must be without constraint, without excessive delay and without excessive expense. The fees should be fixed at a level which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular his right to have the data communicated to him in an intelligible form, and on the other, the burden which the obligation to communicate such data represents for the controller. The fees may not be fixed at a level likely to constitute an obstacle to the exercise of the right of access, and it should not exceed the cost of communicating such data. (¶¶ 22, 25, 28-30)

2.3. ERASURE

Google: A supervisory authority or judicial authority may order a search engine operator to remove a link from a list of results without presupposing the previous or simultaneous removal of the underlying information from the web page on which it was published. Requiring the data subject to obtain erasure from web pages would not provide effective and complete protection of the data subject, especially because publishers may not be subject to EU data protection law or publication may be carried out "solely for journalistic purposes" and thus benefit from the derogation. Further, balancing would be different for processing by a search engine and processing by a web publisher. (¶¶ 82-85)

The search engine operator must erase the information and links concerned in the list of results if that information appears, having regard to all circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine. Here, having regard to the sensitivity for the data subject's private life of the information contained in announcements and the fact that initial publication occurred 16 years before, the data subject has established that the links should be removed. (¶ 98)

3. BALANCING FUNDAMENTAL RIGHTS

3.1. PROTECTION OF PROPERTY AND AN EFFECTIVE REMEDY

Promusicae: The requirements of protection of different fundamental rights must be reconciled, namely the right to respect for private life on the one hand and rights to protection of property and an effective remedy on the other hand. Directive 2002/58 provides rules determining in what circumstances and to what extent personal data processing is lawful and what safeguards must be provided. (¶¶ 65-70)

LSG: The decision refers to ¶ 70 of Promusicae decision regarding balancing fundamental rights. That decision did not rule out the possibility that Member States may place ISP under a duty of disclosure. An ISP provides a service which enables users to infringe copyright by providing the connection. (¶¶ 27, 43)

Scarlet: The injunction to install the contested filtering system did not respect the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual property right

enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information. (¶ 53)

Bonnier: The national legislation in question requires, for an order for disclosure of the data in question to be made, that there be clear evidence of an infringement of an intellectual property right, that the information can be regarded as facilitating the investigation into a copyright infringement and that the reasons for the measure outweigh the potential harm to the person affected. Thus, it enables the national court seised of an application for an order for disclosure of personal data to weigh the conflicting interests involved, and thereby in principle ensures a fair balance between protection of intellectual property rights and protection of personal data. (¶¶ 58-60)

3.2. FREEDOM OF EXPRESSION

Lindquist: Data protection and freedom of expression must be balanced against each other, and the regime of the Directive provides in itself multiple mechanisms allowing a balancing of the different fundamental rights to be carried out. Therefore it is not a disproportionate violation of the principle of freedom of expression. (¶¶ 82-87) 90)

3.3. ACCESS TO DOCUMENTS

Bavarian Lager: The General Court erred in limiting the application of the exception in Article 4(1)(b) to situations in which privacy or the integrity of the individual would be infringed for the purposes of Article 8 of the ECHR and the caselaw of the European Court of Human Rights, without taking into account the legislation of the EU concerning the protection of personal data, particularly Regulation 45/2001. It disregarded the wording of the Article, which is an indivisible provision and requires that any undermining of privacy and the integrity of the individual must always be examined and assessed in conformity with the EU data protection legislation. The Article establishes a specific and reinforced system of protection of a person whose personal data could, in certain cases, be communicated to the public. (¶¶ 58-60)

Recital 15 of Regulation 45/2001 indicates legislative intent that Article 6 TEU and thereby Article 8 ECHR should apply where processing is carried out in the exercise of activities outside the scope of Regulation 45/2001 (Titles V and VI of pre-Lisbon TEU). Such reference was unnecessary for activities within the scope of Regulation 45/2001. Thus, where a request based on Regulation 1049/2001 seeks access to documents including personal data, Regulation 45/2001 becomes applicable in its entirety, including Articles 8 and 18. The General Court erred in dismissing the application of Article 8(b) and 18 of Regulation 45/2001, and its decision does not correspond to the equilibrium which the legislator intended to establish between the two Regulations. (¶¶ 62-65)

The Commission was right to verify whether the data subjects had given their consent to disclosure of personal data concerning them. By releasing the expurgated version of the minutes, with the names of 5 participants removed (three could not be contacted, two objected), the Commission did not infringe Regulation 1049/2001 and complied with its duty of openness. By requiring that regarding these five persons, the applicant establish the necessity for those personal data to be transferred, the Commission complied with the provisions of Article 8(b) of Regulation 45/2001. As no necessity was provided, the Commission was not able to weigh up the various interests of the parties concerned, nor to verify whether there was any reason to assume that the data subjects' legitimate interests might be prejudiced, as required by Article 8(b). (¶¶ 75-78)

Client Earth: Where an application is made seeking access to personal data, the provisions of Regulation 45/2001 (particularly Article 8(b)) become applicable in their entirety. Under Article 8(b), personal data may generally be transferred only if the recipient establishes necessity and if there is no reason to assume that the transfer might prejudice the legitimate interests of the data subject. Thus, the transfer is subject to these two cumulative conditions being satisfied. The applicant must establish the first condition, and the institution must determine whether there is such reason. If there is no such reason, the transfer must be made; if there is such reason, the institution must weigh the various competing interests in order to decide on the request. (¶¶ 44-47)

The consideration that disclosure was likely to undermine the privacy and integrity of the experts concerned is a consideration of a general nature not otherwise supported by any factor specific to the case. Disclosure would have made it possible for suspicions of partiality to be dispelled or

allowed the experts to dispute the merits of those allegations. If a general consideration, unsupported by evidence, were to be accepted, it could be applied to any situation where an EU authority obtains experts opinions, contrary to the requirement that exceptions to the right of access to documents must be interpreted strictly. Thus, the conditions required by Article 8(b) were satisfied. (¶¶ 69-71)

Jordana: Article 4(1)(b) of Regulation 1049/2001 is indivisible, and requires that the violation of private life and the integrity of the individual are always analysed in conformity with the right to protection of personal data. Thus it establishes a specific regime where personal data may be communicated to the public. Since this case concerns the processing of personal data, the request must be analysed under Regulation 45/2001. In rejecting the application for access to documents, the Commission had failed to apply Regulation 45/2001 in its analysis, and thus erred. (¶¶ 99-100)

Dennekamp I: Regulation 1049/2001 and Regulation 45/2001 do not contain any provisions granting one primacy over the other, therefore full application of both should, in principle, be ensured. (¶ 24)

Where a request based on Regulation 1049/2001 seeks access to documents containing personal data, Regulation 45/2001 becomes applicable in its entirety, including Article 8. The applicant cannot claim that the processing he requested was lawful on the basis of Article 5(b) and this suffices, since Article 8(b) applies without prejudice to Article 5. (¶¶ 26-29)

In order to obtain disclosure of the personal data contained in the documents, the applicant would have had to demonstrate, by providing express and legitimate justifications, the necessity for the requested personal data to be transferred, so that the Parliament could weigh up the various interests of the parties concerned and determine whether legitimate interests of MEPs might be prejudiced by the transfer. The applicant failed to establish why he needed the names to obtain his objectives. He did not explain with express arguments and justifications in what respect the transfer of the data was necessary to satisfy the public interest which he invoked, nor that the transfer would have been proportionate to his aims. (¶¶ 26-29)

Further, the Parliament was not required to weigh the interests invoked by the applicant against those of MEPs, or to determine whether there was any reason to assume that the legitimate interests of those MEPs might have been prejudiced by such transfer. Thus, no manifest error that the Parliament might have made in weighing up interests has any bearing in this case on the lawfulness of the decision. (¶ 44)

Article 4(1)(b) is an indivisible provision requiring the institution concerned always to examine and assess any undermining of privacy and the integrity of the individual in conformity with Regulation 45/2001. (¶ 39)

Egan & Hackett: The Parliament systematically took the view that the public should not have access to documents revealing the identity of former MEP assistants. It did not carry out an examination to show that the access would specifically and effectively undermine their privacy within the meaning of the provisions in question, nor did it verify whether the risk of the protected interest being undermined was reasonably foreseeable and not purely hypothetical. Thus, it failed to show to what extent disclosure would specifically and effectively undermine the right to privacy. (¶¶ 89-94)

Dennekamp II: If the applicant has established necessity, and the institution decides there is no reason to assume that data subject's legitimate interests may be prejudiced, the data may be transferred and the documents are to be made available to the public. To fulfill the condition of necessity under that article, an applicant for access to documents containing personal data must establish that the transfer of personal data is the most appropriate of the possible measures for attaining the applicant's objective, and it is proportionate to that objective, which means the applicant must submit express and legitimate reasons to that effect. This strict interpretation cannot be regarded as creating a broad exception to the fundamental right of access to documents which would result in an unlawful restriction of that right. Rather, it reconciles two fundamental yet opposing rights, the institution being required also to examine whether the legitimate interests of the data subjects might be prejudiced by the transfer. The general nature of the justification for transfer has no direct effect on whether the transfer is necessary for the purposes of attaining the applicant's aim. (¶¶ 60-61)

Here, the applicant made two arguments to establish necessity. First, that necessity was based on the right to information and freedom of expression. These are not sufficient to establish that the transfer is the most appropriate of the possible measures for attaining the objective, or that it is proportionate to that objective. Moreover, the applicant did not make clear in what respect transferring the names of the MEPs participating in the scheme was the most appropriate measure for attaining the objective he had set for himself. He merely asserted that the measures designed to provide public control over public expenditure in the context of the additional pension scheme, like the discharge procedure, did not protect the fundamental right to information and to communicate it to the public. From this it cannot be determined in what respect the transfer would be the most appropriate measure, or how it is proportionate. (¶¶ 81-87)

Second, the applicant argued that the transfer of personal data is necessary to determine whether MEPs' voting behavior regarding the additional pension scheme is influenced by their financial interest, and disclosure of all the names of the MEPs participating in the scheme would be the only way for the public to hold its representatives accountable for their actions in relation to the scheme. The court agreed that the transfer is the only measure by which the applicant's aim can be attained; no other measure is capable of ensuring that MEPs facing a potential conflict of interest are identified. Further, it is proportionate for this purpose. (¶¶ 88-94)

The EU institution or body in receipt of the application must refuse the transfer if there is the slightest reason to assume that the data subjects' legitimate interests would be prejudiced. MEPs as public figures have chosen to expose themselves to scrutiny by third parties, particularly the media and general public, even if such choice in no way implies that their legitimate interests must be regarded as never being prejudiced by a decision to transfer their data. Thus, they have generally already accepted that some of their personal data will be disclosed to the public. That must be taken into account when assessing the risk of prejudice to their legitimate interests. Particular consideration should be given to the link between the personal data at issue and their mandate, and to the legal and financial commitment of the EP to the scheme. In view of the importance of the interests invoked here, which are intended to ensure the proper functioning of the EU by increasing the confidence that citizens may legitimately place in the institutions, the legitimate interests of the MEPs who are members of the scheme cannot be prejudiced by the transfer of personal data at issue. (¶¶ 115-131)

An institution which refuses access on the ground of prejudice to legitimate interests must state reasons for invoking such interests. The institution must explain how disclosure of a document could specifically and actually undermine the interest protected by the exception. The explanation cannot consist of a mere assertion that access would undermine privacy. Examination of the specific and actual nature of the undermining of the interest under Article 4(1)(b) of Regulation 1049/2001 is indissociable from the assessment of the risk that the legitimate interests of the data subject referred to in Article 8(b) of Regulation 45/2001 which, through the disclosure to the public, might be prejudiced by the transfer of personal data. (¶¶ 133-135)

McCullough: The applicant cannot be deemed to have proved the necessity of having the personal data at issue transferred. The only justification provided was to supplement his written defence before the Greek Examining Magistrate. Applicant did not provide any information or justification as to how the submission of the requested documents containing that data would affect the Greek proceedings, the risks to which he would be exposed in procedural terms, and the merits of his defence if the documents were not submitted to the Greek Magistrate. (¶¶ 69-70)

Exceptions under Article 4 must be interpreted and applied strictly. An institution refusing access must explain how disclosure of that document could specifically and actually undermine the interest protected by the exception. The fact that a document concerns an interest protected by an exception is not of itself sufficient to justify application of that exception. Rather, it is necessary for the institution to have previously determined (1) that the document would specifically and actually undermine the protected interest and (2) that the risk of the protected interest being undermined is reasonably foreseeable and not purely hypothetical. The institution must explain how granting access to the document could specifically and actually undermine the interest protected by the exception under Article 4(1)(b).

Here, Cedefop simply states that the persons concerned are protected as individuals and any access would lead to a serious violation of the privacy and integrity of the individual as they clearly demonstrated the opinions and views of the members on the subject matters discussed. However, Cedefop neither carried out an examination demonstrating that granting access to those

documents would specifically and actually undermine the privacy of those members within the meaning of Article 4(1)(b), nor verified whether the risk of the protected interest being undermined was reasonably foreseeable and not purely hypothetical. It is not apparent how the opinions and views expressed could fall within the sphere of their privacy, since those meetings were professional. (¶¶ 82-88)

4. TRANSFERS

Lindquist: The publication on the internet did not constitute a transfer, as an internet user would have to connect to the internet and personally carry out the necessary actions to consult those pages. Mrs. Lindquist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access. There is no transfer of data to a third country within the meaning of Article 25 when an individual in a Member State loads personal data onto an internet page which is stored with his/her hosting provider in that or another Member State, thereby making the data accessible to anyone who connects to the internet, including people in a third country. (¶¶ 60-61, 68, 70)

Dennekamp II: Articles 7-9 of Regulation 45/2001 precisely limit the possibility of transferring personal data so as to make it subject to strict conditions which, if not fulfilled, prohibit any transfer. Those conditions always include the necessity of the transfer in the light of various aims. (¶ 58)

4.1. APPROPRIATE LEGAL BASIS

PNR:

- Adequacy decision: Requirements for transfer were based on a statute enacted by the USA in November 2001 and implementing regulations adopted thereunder, which concern enhancement of security and conditions under which persons may enter and leave the USA, fighting against terrorism and transnational crime. Thus, the transfer of PNR data is processing concerning public security. (¶¶ 55-56) Even though PNR data are initially collected in the course of commercial activity, the processing addressed in the adequacy decision concerns safeguarding public security and law enforcement. The facts that the data are collected by private operators for commercial purposes and that those operators arrange for the transfer of the data to a third country does not prevent that transfer from being regarded as processing excluded from the Directive's scope. Thus, it falls within the first indent of Article 3(2) of the Directive, which excludes from the Directive's scope data protection in the course of activities provided for by Titles V and VI of the EU Treaty. Thus the adequacy decision is annulled. (¶¶ 57-61)

- Agreement: Article 95 of the EC Treaty (internal market) in conjunction with Article 25 of the Directive (transfers to third countries ensuring adequacy) do not justify EU competence to conclude the Agreement. The agreement relates to the same transfers as the adequacy decision, and thus processing operations are outside the scope of the Directive. The Council decision approving the conclusion of the agreement between the EU and the US on the processing of PNR data is annulled. (¶¶ 67-70)

4.2. ADEQUATE LEVEL OF PROTECTION

Schrems: The word "adequate" in Article 25(6) signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed by the EU legal order. However, it requires the third country to ensure, by reason of its domestic law or international commitments, a level of protection of fundamental rights and freedoms *essentially equivalent* to that guaranteed by the EU by virtue of Directive 95/46 read in light of the CFR, otherwise that protection could be easily circumvented by transfers. Thus, the legal order of the third country covered by a Commission adequacy decision must have the means to ensure protection essentially equivalent to that guaranteed within the EU. When examining the level of protection afforded by a third country, the Commission must assess the content of the applicable rules resulting from domestic law or international commitments and the practice designed to ensure compliance. Also, in light of the fact that the level of protection ensured by the third country is liable to change, the Commission must, after adopting an adequacy decision, check periodically whether the adequacy finding remains factually and legally justified. Account must be taken of the circumstances that have arisen after the adoption of the decision. The Commission's discretion as to adequacy is reduced and is

subject to strict scrutiny, in view of the important role played by data protection in the light of the fundamental right to respect for private life and the large number of persons potentially concerned by transfers. (¶¶ 73-78)

4.3. SAFE HARBOUR

Schrems: US public authorities are not required to comply with safe harbor principles. Decision 2000/520 specifies that safe harbor principles may be limited to the extent necessary to meet national security, public interest or law enforcement requirements, or statute, regulation or caselaw. Self-certified US organisations receiving personal data from the EU are thus bound to disregard safe harbor principles when they conflict with US legal requirements. Decision 2000/520 does not contain sufficient findings regarding US measures which ensure adequacy by reason of domestic law or international commitments. Rather, it enables interference with fundamental right to respect for private life of persons whose personal data is or could be transferred from the EU to the US. (¶¶ 82-87)

The Decision does not contain any finding regarding US rules intended to limit the interference when they pursue legitimate objectives such as national security, nor refer to effective legal protection against such interference. FTC procedures and private dispute resolution mechanisms concern compliance with safe harbor principles (against US organisations) and cannot be applied with respect to measures originating from the State. Moreover, the Commission found that US authorities could access the personal data transferred and process it in a way incompatible with the purposes for which it was transferred, and beyond what was strictly necessary and proportionate for the protection of national security, and data subjects had no redress regarding their rights of access, rectification and erasure. Legislation permitting public authorities to have generalized access to the content of electronic communications compromises the essence of the fundamental right to respect for private life. Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access, rectification or erasure of his own personal data does not respect the essence of the fundamental right to effective judicial protection. (¶¶ 88-95)

Thus, Article 1 of the Decision does not ensure adequacy and the decision is consequently invalid. (¶ 98)

Articles 1 and 3 are inseparable from 2 and 4 and the annexes, thus the entire Decision 2000/520 is invalid. (¶105)

5. REGULATION 45/2001

5.1. SCOPE

Egan & Hackett: Neither Article 2(3) of Regulation 1049/2001, nor Article 3(2) of Regulation 45/2001, nor any other provision, contains any restriction such as to exclude from their respective scopes documents which were, but are no longer, available. (¶ 74)

5.2. LAWFULNESS

Nikolaou: The leak constitutes unlawful processing in violation of Article 5 of Regulation 45/2001 because it was not authorized by the data subject, not necessary under the other sub-paragraphs and it did not result from a decision by OLAF. Even though OLAF has a margin of discretion on transmissions, here it was not exercised because the leak is an unauthorized transmission. OLAF is best placed to prove how the leak occurred and that the Director of OLAF did not violate his obligations under Article 8(3) of Regulation 1073/99. In the absence of such proof, OLAF (the Commission) must be held responsible. No concrete showing was made of an internal system of control to prevent leaks or that the information in question had been treated in a manner that would guarantee its confidentiality. (¶¶ 206-209)

Publication of the press release was not lawful under Article 5(a) and (b) because the public did not need to know the information published in the press release at the time of its publication, before the competent authorities had decided whether to undertake judicial, disciplinary or financial follow-up. (¶224)

6. DIRECTIVE 95/46

6.1. SCOPE

Rechningshof : Applicability of Directive 95/46 cannot depend on whether the specific situations at issue have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty (free movement of workers). The EU system of data protection has a wide scope, is defined in very broad terms, and does not depend on whether, in every specific case, the processing of personal data has a connection to the free movement between the Member States. A contrary interpretation could make the limits of the field of application of the Directive unsure and uncertain. The system consists of checks and balances in which processing of personal data is subject to a number of conditions and limitations. (¶¶ 42-43)

Lindquist: Loading personal data on an internet page is processing by automatic means. (¶ 25)

Huber: Article 3(2) excludes from the scope of Directive 95/46 the processing of personal data concerning public security, defense, and criminal law activities. Thus, in this case, only processing for a purpose relating to the right of residence and for statistical purposes falls within the scope of Directive 95/46. (¶¶ 44-45)

Tietosuojavaltuutettu: Only two exceptions to scope exist, which are set forth in Article 3(2). The first indent states that security and criminal law are activities of the state. The second indent states that processing by a natural person in the course of a purely personal or household activity concerns activities in the course of private or family life of individuals. Activities (c) and (d) are activities of private companies, and are not within the scope of Article 3(2). A general derogation from application of the Directive in respect of published information would largely deprive the Directive of its effect. Thus activities (a) and (b) are also not within the scope of Article 3(2). (¶¶ 39-49)

Rynes: Video surveillance involving the recording and storage of personal data falls within the scope of the Directive, since it constitutes automatic data processing. (¶ 24)

6.2. LAWFULNESS

ASNEF: The second condition of Article 7(f) of Directive 95/46 (the interests of the controller or recipients must not be overridden by the fundamental rights and freedoms of the data subject) necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the particular case. In relation to the balancing, it is possible to take into consideration the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources. The processing of data appearing in non-public sources necessarily implies that information relating to the data subject's private life will thereafter be known by the data controller and recipients, which is a more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the CFR, and must be properly taken into account in the balancing. However, it is no longer a precision within the meaning of Article 5 if national rules exclude the possibility of processing certain categories of personal data by definitively prescribing the result of the balancing thereby not allowing a different result by virtue of the particular circumstances of an individual case. (¶¶ 40-47)

Google: The non-compliant nature of processing may arise from a breach of any conditions of lawfulness imposed by the directive, including data quality and legitimacy. Here, the grounds for legitimacy were those in Article 7(f), which permits processing where necessary for the purposes of the legitimate interests pursued by the controller or third party to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights of the data subject, requiring a balancing of interests. The balancing provided in Article 14 allows account to be taken of all circumstances surrounding data subject's particular situation. (¶¶ 70-75)

- Interest of the data subject: search of an individual's name enables any internet user to obtain through a list of results a structured overview of the information relating to the data subject that can be found on the internet, potentially concerning a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or only with great difficulty, therefore enabling a detailed profile. The interference with the

rights of the data subject are heightened because of the important role played by the internet and search engines in modern society. (¶ 80)

- Interests of search engine: These are economic interests, which cannot justify the potential seriousness of the interference with the data subject 's rights. (¶ 81)

- Interests of internet users: The data subject's rights generally override those of internet users, but the balance may depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, which may vary by the role played by the data subject in public life. The interference may be justified by the preponderant interests of the general public in having access to the information. (¶ 81)

6.3. ESTABLISHMENT OF THE CONTROLLER

Google: Google Spain, a subsidiary of Google Inc. on Spanish territory, is an "establishment" within the meaning of Article 4(1)(a) because it engages in the effective and real exercise of activity through stable arrangements in Spain. (¶ 49)

The processing of personal data by the controller is also "carried out in the context of the activities" of an establishment, even though Google Spain is not involved in the processing at issue (carried out exclusively by Google Inc.) but rather only in advertising in Spain. Article 4(1)(a) does not require that the processing in question be carried out "by" the establishment concerned, but only "in the context of the activities" of the establishment. In light of objective of effective protection of fundamental rights, those words cannot be interpreted restrictively. The activities of the search engine and those of its establishment in the Member State are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine economically profitable and that engine is the means enabling those activities to be performed. (¶¶ 52-56, 60)

Weltimmo: Article 4(1)(a) of Directive 95/46 permits the application of data protection law of a Member State other than the Member State in which the controller is registered, insofar as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity, even minimal, in the context of which the processing is carried out. To establish whether the controller has an establishment in that Member State, both the degree of stability of the arrangements and the effective exercise of activities in the other Member State must be interpreted in light of the specific nature of the economic activities and provision of services concerned, particularly for undertakings offering services exclusively over the internet. The presence of only one representative can suffice to constitute a stable arrangement if he/she acts with a sufficient degree of stability through the presence of the necessary equipment for the provision of the specific services concerned in the Member State. Further, the concept of "establishment" extends to any real and effective activity, even a minimal one, exercised through stable arrangements. (¶¶ 28-31)

Here, the activity of the controller consists in the running of property dealing websites concerning properties in Hungary and written in Hungarian and thus pursues a real and effective activity in Hungary. Further, it has a representative in Hungary responsible for recovering the debts resulting from that activity and representing the controller in administrative and judicial proceedings relating to the processing of the data concerned. It has a bank account in Hungary intended for the recovery of debts and uses a letter box in Hungary for the management of everyday affairs. That is capable of establishing the existence of an "establishment". (¶¶ 32-33)

The processing is done in the context of the activities which Weltimmo pursues in Hungary. Thus Hungarian data protection law would apply with respect to that processing. (By contrast the nationality of the persons concerned by such data processing is irrelevant.) (¶¶ 38-40)

6.4. INDEPENDENCE OF DPA

Germany: Independence normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure. There is nothing to indicate that the requirement of independence concerns exclusively the relationship between the supervisory authorities and the bodies subject to that supervision. The adjective

"complete" implies a decision-making power independent of any direct or indirect external influence on the supervisory authority. The guarantee of independence of DPAs is intended to ensure the effectiveness and reliability of the supervision of compliance with data protection provisions, to strengthen the protection of individuals and bodies affected by their decisions. DPAs must act impartially and must remain free from any external influence, including that of the State or Lander. Independence precludes not only any influence exercised by supervised bodies, but also any directions or other external influence which could call into question the performance of those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data. (¶¶ 18-19, 25, 30)

State scrutiny in principle allows the government of the respective Land to influence the decision of the supervisory authority or cancel and replace those decisions. This is not consistent with the principle of independence.

Austria: By failing to take all measures necessary to ensure that the Austrian national legislation meets the requirement of independence with regard to the DSK, Austria has failed to fulfil its obligations under the second subparagraph of Article 28(1) of Directive 95/46 and Article 8(3) of the Charter of Fundamental Rights of the EU and Article 16(2) TFEU. The establishment in Member States of independent supervisory authorities is thus an essential component of the protection of individuals with regard to the processing of personal data.

The words "with complete independence" must be given an autonomous interpretation. Supervisory authorities must enjoy an independence with allows them to perform their duties free from external influence, direct or indirect, which is liable to have an effect on their decisions. The fact that the DSK has functional independence insofar as its members are "independent and [are not] bound by instructions of any kind in the performance of their duties" is an essential, but not sufficient, condition to protect it from all external influence. (¶¶ 41-42)

Here, the national legislation provides only for the operational autonomy of the supervisory authority, but does not preclude the DSK from performing its duties free from all indirect influence, for the following reasons:

The managing member of the DSK need not always be an official of the Federal Chancellery (although it always has been), and all day-to-day business is thus de facto managed by a federal official, who remains bound by the instructions issued by his employer and is subject to supervision. It is conceivable that the evaluation of the managing member by his hierarchical superior for the purposes of encouraging his promotion could lead to a form of "prior compliance". Moreover, the Chancellery is subject to the supervision of the DSK, so the DSK is not above all suspicion of partiality. The service-related link between the managing member of the DSK and the Chancellery affects the DSK's independence. The fact that the appointment of the managing member rests on an autonomous decision of the DSK does not protect the independence; (¶¶ 45-55)

The office of the DSK is structurally integrated with the departments of the Federal Chancellery, and all DSK staff are under the authority of the Federal Chancellery and subject to its supervision. The DSK need not be given a separate budget to satisfy the criterion of independence. The DPA may come under a specified ministerial department. However, the attribution of the necessary equipment and staff to DPAs must not prevent them from acting with complete independence. Here, since they are subject to supervision by the Chancellery, it is not compatible with the requirement of independence. (¶¶ 56-61)

The Federal Chancellor has the right to be informed of all aspects of the work of the DSK. This precludes the DSK from operating above all suspicion of partiality. (¶¶ 62-63)

Hungary: Establishment in Member States of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of personal data. Operational independence of supervisory authorities, in that members are not bound by instructions of any kind in the performance of their duties, is an essential condition that must be met to respect the independence requirement, but this is not sufficient. The mere risk that the state could exercise political influence over decisions of supervisory authorities is enough to hinder independence. If it were permissible for the Member State to compel the supervisory authority to vacate office before serving full term, even if this comes about as a result of restructuring or changing of the institutional model, the threat of such premature termination could lead the

supervisory authority to enter into a form of prior compliance with the political authority, which is incompatible with the requirement of independence, and the supervisory cannot be regarded as being able to operate above all suspicion of partiality. Member States are free to adopt or amend the institutional model they consider most appropriate for supervisory authorities. However, they must ensure that the independence of the authority is not compromised, which entails the obligation to allow that authority to serve its full term. (¶¶ 51-55, 60)

Schrems: The Directive seeks to ensure an effective, complete, and high level of protection of the fundamental rights and freedoms of natural persons. The guarantee of the DPA's independence is intended to ensure effectiveness and reliability of the monitoring of compliance, and is an essential component of data protection. (¶¶ 40-47)

6.5. DPA POWERS

Weltimmo: In the event that the Hungarian DPA should consider that Weltimmo has an establishment not in Hungary, but in another Member State, then in accordance with Article 28(4), it may exercise its powers conferred under Article 28(3) only within its own territory, and it may, irrespective of the applicable law and before even knowing which national law is applicable, thereby investigate the complaint. If it becomes apparent that it is the law of another Member State that applies, that DPA cannot impose penalties outside the territory of its own Member State. In fulfilment of the duty of cooperation laid down in Article 28(6), it requests the DPA of that Member State to establish an infringement of its national law and impose penalties if that law permits, based on the information which the first DPA has transmitted to second DPA. The second DPA may also find it necessary to carry out other investigations, on the instructions of the first DPA. (¶¶ 44-58)

Schrems: DPAs powers extend to their own Member State, but not to processing in third countries. However, DPAs are responsible for monitoring transfers from a Member State to a third country, as the transfer is processing carried out in the Member State. (¶¶ 40-47)

An adequacy decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46 is addressed to the Member States, which must take the necessary measures to comply with it. Until the Commission decision is declared invalid by the ECJ, it has legal effect in the Member States. However, the Commission decision cannot eliminate or reduce the powers of the DPA accorded by Article 8(3) of the CFR, and therefore cannot prevent data subjects whose personal data has been transferred from lodging a claim pursuant to Article 28(4) with the DPA alleging that an adequate level of protection is not ensured in that third country, which in essence challenges the validity of the Commission's adequacy decision. But the ECJ alone has jurisdiction to declare that the decision is invalid; neither the DPA nor a national court may do so. The latter must refer the claim to the ECJ for a preliminary ruling to examine the validity of the Commission decision. (¶¶ 51-64)

Article 3 of Decision 2000/520 lays down specific rules regarding DPA's powers in light of a Commission adequacy finding (to suspend data flows to self-certified US organisations under restrictive conditions establishing a high threshold for intervention). It excludes the possibility of DPA's taking action to ensure compliance with Article 25 (adequacy), in particular, it denies DPAs powers which they derive from Article 28 to consider a data subject's claim which puts into question whether a Commission adequacy decision is compatible with protection of privacy and fundamental rights and freedoms of individuals. This goes beyond the power conferred on the Commission in Article 25(6). Thus, Article 3 is invalid. (¶¶ 100-104)

6.6. PROCESSING FOR SOLELY JOURNALISTIC PURPOSES

Tietosuojavaltuutettu: Article 1 of the Directive indicates that the objective is that Member States should, while permitting the free flow of personal data, protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy, with respect to processing of their personal data. That objective can only be pursued by reconciling those fundamental rights with the fundamental right to freedom of expression. Article 9's objective is to reconcile the two rights. Member States are required to provide derogations in relation to the protection of personal data, solely for journalistic purposes or artistic or literary expression, which fall within the fundamental right to freedom of expression, insofar as necessary for reconciliation of the two rights. To take account of the importance of the right of freedom of expression in every democratic society, it is necessary to interpret notions of freedom, such as journalism, broadly. Derogations must apply only insofar as strictly necessary. The fact that publication is done for profit making

purposes does not preclude publication from being considered as "solely for journalistic purposes." The medium used is not determinative of whether it is "solely for journalistic purposes." Thus activities may be classified as "journalistic" if their sole object is the disclosure to the public of information, opinions or ideas, irrespective of the medium used to transmit them. (¶¶ 52-56, 59, 61)

6.7. PROCESSING FOR PURELY PERSONAL OR HOUSEHOLD ACTIVITY

Lindquist: Mrs. Lindquist's activities were mainly charitable and religious, but these are not covered by the exceptions in Article 3(2) of the Directive and cannot be considered exclusively personal or domestic. (¶¶ 45-47)

Rynes: Protection of the fundamental right to private life guaranteed under Article 7 of the CFR requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. Also, the wording of the derogation refers to "purely" personal or household activity, not simply a personal or household activity. Correspondence and the keeping of address books constitute, in the light of recital 12 to Directive 95/46, a purely personal or household activity, even if they incidentally concern the private life of other persons. However, to the extent that video surveillance covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data, it cannot be regarded as a purely personal or household activity. In such case, the consent of the data subject would be required to process his data. (¶¶ 28-35)

6.8. TRANSPOSITION/HARMONISATION

Luxembourg: A Member State may not plead provisions, practices or circumstances in its internal legal system (here, the new distribution of ministerial powers following a change in its internal government) in order to justify a failure to comply with obligations and time limits laid down in a Directive, and thus a violation had occurred relating to the transposition of Directive 95/46. (¶¶ 8-9)

Lindquist: The Directive envisages complete harmonization, thus Member States must adopt national legislation conforming to the regime of the Directive. However, certain provisions of the Directive can explicitly authorize the Member States to adopt more constraining regimes of protection. This must be done in accordance with the objective of maintaining a balance between free movement of personal data and protection of private life. In addition, Member States remain free to regulate areas excluded from the scope of application of the Directive in their own way, provided no other provision of EU law precludes it. (¶¶ 96-99)

Promusicae: Directives 2000/31, 2001/29, 2004/48 and 2002/58 do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in civil proceedings, nor does it oblige them to impose such an obligation. However, when transposing various intellectual property Directives, Member States must take care to interpret them such that there is a fair balance struck between the various fundamental rights protected by the Community legal order. Further, when implementing the national law transposing those Directives, authorities and courts of the Member States must interpret them in a manner consistent with the Directives and make sure that the interpretation does not conflict with those fundamental rights or other general principles of Community law, such as the proportionality principle. (¶ 70)

ASNEF: Harmonisation of national laws is not limited to minimal harmonisation but harmonisation which is generally complete. Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of data subjects, equivalent in all Member States. Consequently, Article 7 of Directive 95/45 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as lawful. That interpretation is corroborated by the term "may be processed only if" which demonstrates the exhaustive and restrictive nature of the list appearing in that Article. Thus the Member States cannot add new principles relating to the lawfulness of processing or impose additional requirements. (¶¶ 29-32)

Article 5 authorises Member States to specify the conditions under which the processing of personal data is lawful, within the limits of Article 7, inter alia. That margin of discretion can be used only in accordance with the objective pursued by the Directive of maintaining a balance between the free

movement of personal data and the protection of private life. A distinction must be made between national measures that provide for additional requirements amending the scope of a principle referred to in Article 7 (precluded) and national measures which provide for a mere clarification of one of those principles (allowed). Thus, Article 7(f) precludes any national rules which, in the absence of the data subject's consent, impose requirements that are additional to the two cumulative conditions set out in that Article (¶¶ 33-39)

Englebert: Article 13(1) states "Member States may" and thus does not oblige the Member States to lay down in their national law exceptions for the purposes listed therein. Rather they have the freedom to decide whether, and for what purposes, to take legislative measures aimed at limiting the extent of the obligations to inform the DS. Further, they may take such measures only when necessary. (¶ 32)

6.9. DIRECT APPLICABILITY

Rechnungshof: Wherever provisions of a directive appear to be unconditional and sufficiently precise, they may, in the absence of implementing measures adopted within the prescribed period, be relied on against any incompatible national provision, or insofar as they define rights which individuals are able to assert against the State. (¶ 98)

ASNEF: Whenever the provisions of a Directive appear to be unconditional and sufficiently precise, they have direct effect if the Member State has failed to implement that Directive in domestic law by the end of the prescribed period. Article 7(f) is sufficiently precise, as it states an unconditional obligation. (¶¶ 52-55)

7. DIRECTIVE 2002/58

7.1. SCOPE

Bonnier: The communication of name and address of a person using an IP address from which files were shared (for copyrighted audio books) falls within the scope of Directive 2002/58 (and within the scope of Directive 2004/48, dealing with copyright). (¶¶ 52-54)

7.2. TRAFFIC DATA

Probst: Article 6(2) of Directive 2002/58 provides an exception to the confidentiality of communications, stating that traffic data necessary for purposes of subscriber billing and interconnection payments may be processed "up to the end of the period during which the bill may lawfully be challenged or payment pursued". Thus, the provision covers the processing necessary for securing payment, including debt collection. (¶ 17)

Article 6(5) provides that traffic data processing authorized by Article 6(2) "must be restricted to persons acting *under the authority of* [service] providers of the public communications networks and publicly available electronic communications services handling billing" and "must be restricted to what is necessary" for the purpose of such activity. Thus, the assignee of claims for payment is authorized to process the data on condition that it acts "under the authority" of the service provider and that it processes only traffic data which are necessary for the purpose of recovery of those claims. That provision seeks to ensure that such externalization of debt collection does not affect the level of protection of personal data enjoyed by the user. "Under the authority" must be strictly construed to mean that the assignee acts only on instructions and under the control of the service provider. The contract between the service provider and assignee must contain provisions ensuring the lawful processing of traffic data by the assignee and must allow the service provider to ensure at all times that those provisions are being complied with by the assignee. (¶¶ 18-27)

8. DIRECTIVE 2006/24

8.1. APPROPRIATE LEGAL BASIS

Ireland: The Court rejected Ireland's argument that the sole or principal objective of the Directive 2006/24 is the investigation, detection and prosecution of crime. Article 95(1) provides that the Council is to adopt measures for approximation of provisions laid down by law, regulation or

administrative action in the Member States which have the objective of establishment and functioning of the internal market. It may be used where disparities exist (or are likely to exist in the future) between national rules which obstruct fundamental freedoms or create distortions of competition and thus have a direct effect on the functioning of the internal market. The premise of the Directive was to harmonize disparities between national provisions governing retention of data by service providers, particularly regarding the nature of data retained and periods of data retention. It was apparent that differences were liable to have a direct impact on the functioning of the internal market which would become more serious with the passage of time. (¶¶ 62-71)

Article 47 of the EU Treaty provides that none of the provisions of the EC Treaty may be affected by a provision of the EU Treaty, in order to safeguard the building of the *acquis communautaire*. Insofar as Directive 2006/24 comes within the scope of Community powers, it could not be based on a provision of the EU Treaty without infringing Article 47. Directive 2006/24 provisions are limited to activities of service providers and do not govern access to data or use thereof by police or judicial authorities of the Member States. They are designed to harmonize national laws on the obligation to retain data, the categories of data to be retained, the periods of retention of data, data protection and data security, and the conditions for data storage. They do not involve intervention by police or law enforcement authorities of Member States, nor access, use or exchange by them. Thus Directive 2006/24 relates predominantly to functioning of the internal market. (¶¶ 75, 78, 80-83)

8.2. SCOPE

Bonnier: Directive 2006/24 deals exclusively with handling and retention of data generated by electronic communication service providers for the purpose of the investigation, detection, and prosecution of serious crime and their communication to competent national authorities. Thus a national provision transposing the EU intellectual property directive which permits an ISP in civil proceedings to be ordered to give a copyright holder information on the subscriber to whom the ISP provided an IP address allegedly used in an infringement is outside the scope of Directive 2006/24 and therefore not precluded by that Directive. It is irrelevant that the Member State concerned has not yet transposed Directive 2006/24. (¶¶ 40-41)

8.3. LAWFULNESS

DRI: The material objective of Directive 2006/24 is of general interest – to ensure data are available for the purpose of the investigation, detection and prosecution of serious crime, and therefore to public security, and international terrorism. (Article 6 CFR lays down the right of any person to liberty and security.) Data relating to use of electronic communications are particularly important and a valuable tool in the prevention of offences and the fight against crime. (¶¶ 41-44)

The proportionality principle requires that acts of EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation and do not exceed the limits of what is appropriate and necessary to achieve those objectives. Given the important role played by data protection in light of the fundamental right of privacy, and the extent and seriousness of the interference (of Directive 2006/24), the EU legislature's discretion is reduced, thus the review of that discretion should be strict. Retention of data is an appropriate tool for the objective pursued. (¶¶ 46-49)

The fight against serious crime and terrorism is of utmost importance to ensure public security and its effectiveness may depend on the use of modern investigation techniques. But this does not, in itself, justify the retention measure being considered to be necessary. Derogations and limitations in relation to data protection must apply only insofar as strictly necessary. Here, the legislation must lay down clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of the data. The need for safeguards is all the greater where personal data are subjected to automatic processing and there is significant risk of unlawful access to the data. Further, the Directive requires retention of all traffic data concerning fixed telephony, mobile telephony, internet access, internet e-mail and internet telephony – i.e. all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. It covers all subscribers and registered users – and therefore entails an interference with the fundamental rights of practically the entire European population. It does not mandate any link to crime. (¶¶ 51-58)

Directive 2006/24 fails to lay down objective criteria by which to determine the limits of access of competent national authorities to the data and its use, nor substantive and procedural conditions relating to access by competent national authorities and to their subsequent use. It does not lay down objective criteria to limit the number of persons authorized to have access and use to what is strictly necessary, and is not made dependent on prior review carried out by a court or independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of obtaining the objective pursued. (¶ 62)

The Directive establishes retention period of a minimum of 6 months and a maximum of 24 months, but it does not state that determination of the exact period must be based on objective criteria to ensure that it is limited to what is strictly necessary. (¶¶ 63-64)

The Directive does not provide for sufficient safeguards to ensure effective protection of the data retained against the risk of abuse and unlawful access. It does not lay down rules adapted to the vast quantity of data whose retention is required, the sensitive nature of that data, and the risk of unlawful access, nor is there a specific obligation set on Member States to establish such rules. Rather, it permits providers to have regard to economic considerations when determining the level of security. (¶¶ 66-67)

The Directive does not require that the data be retained within the EU, with the result that it cannot be held that the control by an independent authority of compliance with the requirements of data protection and security is fully guaranteed. This is an essential component of protection of individuals with regard to the processing of personal data. (¶ 68)

Accordingly, the EU legislature exceeded limits imposed by compliance with principle of proportionality in light of Articles 7, 8 and 52(1) CFR. (¶ 69)

9. ARTICLES 7, 8 CFR

Schecke: The validity of legislation requiring publication must be assessed in light of provisions of the CFR, including Article 8. However, CFR Article 52(1) accepts that limitations may be imposed on rights under the CFR, as long as they are provided by law, respect the essence of those rights and are proportionate (necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others). Further, CFR Article 52(3) states that for rights in the CFR which correspond to rights in the ECHR, the meaning and scope shall be the same as for the ECHR. (¶¶ 46-51)

Publication must a) be provided by law, b) respect the essence of the rights and freedoms in CFR Arts. 7 and 8, and c) be proportionate (necessary and genuinely meet the objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others). Here, publication is lawful since it is specifically provided for by the Regulation. It meets the general interest requirement because publication is intended to enhance transparency regarding the use of CAP funds and sound financial management. Regarding proportionality, it is necessary to analyse whether the EU balanced its interest in guaranteeing transparency and ensuring best use of public funds with the rights of beneficiaries to privacy and data protection. Derogations to data protection are allowed only insofar as strictly necessary. (¶¶ 66-77)

For natural persons, there is nothing to show that lawmakers made an effort to strike a balance. No automatic priority can be conferred on the objective of transparency over data protection, even if important economic interests are at stake. Thus, the lawmaker exceeded the limits which the proportionality principle imposes. (¶¶ 80-85)

Publication of the data in question with respect to the complainant legal person does not go beyond limits imposed by the proportionality principle. The seriousness of the breach manifests itself in different ways for legal persons versus natural persons. It would impose an unreasonable administrative burden on the competent national authorities if they were obliged to examine, before the data are published for each legal person who is a beneficiary, whether the name of that person identifies natural persons. Thus, the legislation requiring publication is valid with respect to the legal persons. (¶¶ 87-88)

Schwartz: Taking and storing of fingerprints by national authorities, governed by Article 1(2) of Regulation 2252/2004, constitutes a threat to rights of respect for private life and protection of personal data. (¶ 30)

Article 52(1) allows for limitations on exercise of rights in Arts. 7 & 8 as long as limitations are provided for by law, respect the essence of those rights, and respect proportionality (necessary and genuinely meet objectives of general interest recognised by EU or need to protect rights and freedoms of others). Here, the taking of fingerprints for passports is provided by Regulation 2252/2004 to prevent falsification of passports and prevent fraudulent use thereof, to prevent illegal entry into EU, therefore it pursues an objective of general interest recognised by the EU. (¶¶ 34-38)

DRI: Directive 2006/24 does not permit retention of content, but it might have an effect on the use of the means of communication and consequently on the exercise of freedom of expression guaranteed by Article 11 CFR. It also directly affects private life (guaranteed by Article 7 CFR) and constitutes processing of personal data (and therefore falls under Article 8 CFR).

The obligation on providers of publicly available electronic communications services or public communications networks to retain data relating to a person's private life and his communications in itself constitutes an interference with Article 7. Access of competent national authorities to the data constitutes a further interference with that right. The Directive constitutes an interference with Article 8 because it provides for processing of personal data. The interferences with Articles 7 and 8 are wide-ranging and particularly serious. The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of users the feeling that their private lives are the subject of constant surveillance. (¶¶ 29, 32, 34-37)

Any limitation on the exercise of rights and freedoms laid down by the CFR must be provided by law, respect their essence and, subject to principle of proportionality, limitations may be made to those right and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others. Even though retention constitutes a particularly serious interference with the right to privacy, it is not such as to adversely affect the essence of those rights given that the Directive does not permit the acquisition of knowledge of the content of the electronic communications. Nor does it adversely affect the essence of the right to protection of personal data because certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or public communications networks – to ensure appropriate technical and organizational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data. (¶¶ 38-40)

Schecke: Publication on the website of data naming beneficiaries and amounts they receive constitutes interference with private life under CFR Article 7. It is irrelevant that data concerns activities of a professional nature, as under Article 8 ECHR, as the CFR has held that no principle justifies exclusion of activities of a professional nature from the notion of private life. (¶¶ 58-59)

10. ARTICLE 8 ECHR

Rechnungshof: The provisions of Directive 95/46, insofar as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must be interpreted in light of that right, which forms an integral part of the general principles of EU law. Article 8 ECHR states that public authorities must not interfere with the right to respect for private life, unless it is in accordance with law and is necessary in a democratic society to protect certain interests. (¶¶ 70-71)

The collection of data by name relating to an individual's professional income, with a view to communicating it to third parties, falls within the scope of Article 8. The ECtHR has held that communication of the data infringes the right of the persons concerned to respect for private life. (¶¶ 73-74)

Regarding necessity, the purpose of the provision was to keep salaries within reasonable limits, which fits within the "economic well-being of the country". But "necessary" means that a pressing social need is involved and the measure is proportionate to the legitimate aim pursued. The authorities enjoy a margin of appreciation. The interests of the state must be balanced against the

seriousness of the interference. The interference is justified only insofar as publication of the names is both necessary and appropriate to the aim of keeping salaries within reasonable limits, which is for the national court to examine. If not, then the interference also constitutes a violation of Articles 6 and 7 of Directive 95/46. (¶¶ 82-90, 94)

V: Article 8 ECHR on private life relates to a fundamental right which covers the right to secrecy of one's medical state. The transfer of that data to a third party, even another EU institution, is an interference with that right, whatever the final use. Such interference may be justified if it is "in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." (¶¶ 113, 123)

Regulation 45/2001 establishes that inter-institutional transfers are foreseen. However, Article 7 is very general. Further, Article 6 states that personal data shall only be processed for purposes other than those for which they were collected if the change of purpose has been expressly foreseen by the rules of the EU institution, which was not the case here. (¶¶ 115-119)

The criterion "necessary in a democratic society" is met if it is necessary to respond to a social imperative, and if it is proportionate to the legitimate end and the reasons specified are relevant and sufficient. The national authority has a limited margin of discretion. The right to privacy of medical data is protected by the EU juridical order, not only to protect the private life of the sick but also to preserve their confidence in the medical body and the medical services in general. The possibility to transfer such data to another institution calls for a particularly rigorous examination. Thus the interest of the Parliament to recruit a person able to exercise his duties must be balanced against the gravity of the interference of the right of the person concerned. The interest of the Parliament to conduct the medical examination does not justify the transfer without the consent of the person concerned. The data are very sensitive, were collected nearly two years before, for a specified purpose, by an institution for which the applicant did not work. The need of the Parliament could have been met by less intrusive means. (¶¶ 122-127)

Article 1 specifies that EU institutions protect the fundamental rights of natural persons, in particular their right to privacy with respect to processing their personal data. Thus, the provisions of the Regulation may not be read as legitimising an interference to the right to privacy. The purpose for the Commission's collection of the data was to determine the applicant's fitness to perform the duties in the Commission's post. Using them to determine her fitness for the post with the Parliament constituted a change of purpose. Each institution is an independent employer, and is autonomous in the management of its personnel. The change of purpose was not foreseen in any legal text. (¶¶ 128-136)