INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES (IRISS)

COORDINATED BY DR. REINHARD KREISSL
IRKS INSTITUT FÜR RECHTS- UND KRIMINALSOZIOLOGIE
WEIN, AUSTRIA

DELIVERABLE D5: EXERCISING DEMOCRATIC RIGHTS UNDER SURVEILLANCE REGIMES

LED BY PROFESSOR CLIVE NORRIS AND DR XAVIER L'HOIRY
DEPARTMENT OF SOCIOLOGICAL STUDIES
UNIVERSITY OF SHEFFIELD, UK

A EUROPEAN PERSPECTIVE ON DATA PROTECTION AND ACCESS RIGHTS

ANTONELLA GALETTA & PROFESSOR PAUL DE HERT
VRIJE UNIVERSITEIT BRUSSEL, BELGIUM

A EUROPEAN PERSPECTIVE ON DATA PROTECTION AND ACCESS RIGHTS

Introduction

The EU Data Protection Directive of 1995 (Directive 95/46/EC)[1] is the main legislative instrument that regulates the processing of personal data at European level. It applies to all 27 Member States of the Union which have implemented the Directive, as well as to the European Economic Area (EEA), which includes Iceland, Liechtenstein and Norway. Data protection is currently undergoing a significant reform process which was triggered by the 2012 European Commission proposal for a Regulation "on the protection of individuals with regard to the processing of personal data and on the free movement of such data"[2] and the proposal for a Directive "on the protection of individuals with regard to the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data"[3]. This Section outlines the European legal framework concerning data protection, in particular focus on subject access rights.

Key principles and concepts of the EU Data Protection Directive

The current European data protection norms date back to 1995, when the main imperatives of the EU were economic integration, harmonisation and the establishment of a European internal market. The 1995 Directive was designed within the pillar-structure of the European Community, where the boundary between Community law (the 'first pillar'), foreign affairs and common security (the 'second pillar'), and justice and internal affairs (the 'third pillar') was sharp and indeed was supposed to be so[4]. Accordingly, having its roots in the European first-pillar law, the Directive emphasised the processing and free movement of personal data, in an attempt to regulate these practices. Although the protection of individuals with regard to the processing of personal data is an important purpose of the Directive, it cannot be considered as its main priority. In the Directive, the needs of state bureaucracies and private business to collect, store and analyse data is given even greater emphasis. This aspect will be highlighted in the sections and paragraphs that follow.

Despite its limitations, Directive 95/46/EC can be considered as a milestone towards the emergence of data protection as a fundamental citizen right in the EU.[5] Before 1995,

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

[2] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, Brussels, 25 January 2012.

[3] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigations, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (General Data Protection Directive), COM(2012) 10 final, Brussels, 25 January 2012.

[4] Rosamond, Ben, *Theories of European integration*, Hampshire: Palgrave, 2000. Dinan, Desmond, *Ever Closer Union?: An introduction to European integration*, Basingstoke : Palgrave Macmillan, 2010.

[5] Gonzales Fuster, Gloria and Raphaël Gellert, "The fundamental right of data protection in the European Union: in search of an uncharted right", *Review of Law, Computers & Technology*, Vol. 26, No. 1, 2012, pp. 73-82.

provisions on data protection were basically left to national initiatives.[6] Nonetheless, the way towards the establishment of a European legal framework on data protection was paved by the Organisation for Economic Cooperation and Development (OECD) Guidelines of 1980[7] and by the Council of Europe Convention 108 "for the protection of individuals with regard to automatic processing of personal data" of 1981[8]. Since then, the fundamental right to data protection has developed autonomously in European law through the case law of the European Courts of Luxembourg (Court of Justice of the European Union, ECJ) and Strasbourg (European Court of Human Rights, ECtHR), with a strong legitimation descending from Art. 8 of the European Convention on Human Rights (ECHR). In more recent times data protection has found a new legal legitimation within the Charter of Fundamental Rights of the European Union which recognises explicitly the right to the protection of personal data (Art. 8)[9]. Remarkably, the second paragraph of Art. 8 of the Charter states, among other things, that "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". It is important here to stress that Art. 8, like any other article of the Charter, has the same legal value as any provision contained in EU treaties.

Directive 95/46/EC had been significantly influenced by the legal developments that took place between the 1970s and 1980s. Indeed, its key principles and provisions recall the OECD Guidelines and especially Convention 108. The OECD Guidelines identify eight "basic principles" that govern data protection, namely: collection limitation principle (1); data quality principle (2); purpose specification principle (3); use limitation principle (4); security safeguards principle (5); openness principle (6); individual participation principle (7); accountability principle (8). Principle number 7 entitles the data subject to exercise the following rights:

1. Right to obtain from the data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
2. Right to have communicated to him data relating to him within a reasonable time, at a charge (if any) that is not excessive, in a reasonable manner and in a form that is intelligible to him;
3. Right to be given reasons if a request is denied and to be able to challenge such denial;
4. Right to challenge data relating to him and to have data erased, rectified, completed or amended.

Chapter II of the Council of Europe Convention 108 (Art. 4-11) established for the first time in European history principles referring to the quality of data and to data processing. In the word of Art. 5, data undergoing automated processing must be:

1. "obtained and processed fairly and lawfully;
2. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

[6] The German federal state of Hessen adopted for the first time a data protection act in 1970. It was then followed by Sweden in 1973 and France in 1978.

[7] OECD Recommendation concerning Guidelines governing the protection of privacy and transborder flows of personal data of 23 September 1980. The Guidelines were not legally binding for OECD member countries.

[8] Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, 1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (last accessed 5 June 2013). Convention 108 was the first legally binding international instrument in the area of data protection.

[9] Charter of Fundamental Rights of the European Union, *Official Journal of the European Union* C 83, 30.3.2010, 389-403. The first paragraph of Art. 8 of the Charter reads as follows: "Everyone has the right to the protection of personal data concerning him or her".

3. adequate, relevant and not excessive in relation to the purposes for which they are stored;
4. accurate and, where necessary, kept up to date;
5. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored".

Derogation from these principles is allowed in specific circumstances only, provided by national law. Exceptions must also constitute necessary measures in a democratic society, "in the interests of protecting state security, public safety, monetary interests or the suppression of criminal offences or the protection of the data subject or the rights and freedoms of others. Furthermore, Convention 108 set out additional safeguards in order to protect "special categories of data" (Art. 6), revealing racial origin, political opinions, religious or other beliefs, as well as personal data concerning health, sexual life or criminal convictions (also known as "sensitive data"). Finally, it emphasised the need to ensure data security (Art. 7) protecting them against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Confirming the apparent continuity between Convention 108 and Directive 95/46/EC, those principles have been endorsed by Directive 95/46/EC. In fact, its Art. 6 spells out the five principles mentioned above. The Directive fixes also 6 criteria for making data processing legitimate (Art. 7), as follows:

1. the data subject has unambiguously given his consent;[10]
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection and of privacy in particular.

Similarly, the Directive ensures special protection to sensitive data (Art. 8) and identifies specific cases in which its provisions do not apply. In particular, the processing of data by a natural person in the course of a purely personal or household activity does not fall within the scope of the Directive, as well as processing activities conducted in the framework of former second and third pillar (Art. 3, Paragraph 2).

[10] Directive 95/46/EC does not clarify in which circumstances consent is considered to be unambiguous. According to the European Data Protection Supervisor (EDPS), unambiguous consent has to be given freely, must be specific and there has to be no doubt as to whether it was given or not". EDPS, Legitimate reasons for processing of personal data, https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA6 (last accessed 7 January 2014). The Article 29 Working Party points out that "only consent that is based on statements or actions to signify agreement constitutes valid consent", Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 13 July 2011, p. 2.

Three main features characterise the legal design of Directive 95/46/EC. First, the Directive adopts a cautious approach when establishing norms and exceptions to the norms, so that to reach a sound balance between privacy and fundamental rights on one hand and the free movement of data on the other. Second, the Directive put emphasis on the relationship between the data controller and the data subject, defining their reciprocal position and rights. Third, the Directive gives Member States a certain margin of manoeuvre in having a final say on the effective application of its provisions, such as in the case of Art. 8, Paragraph 2, a) and b)[11]. This ambiguity can also be found in expressions such as "state security" (Art. 3, Paragraph 2); "public interest" (Art. 7, Paragraph e)); "vital interests of the data subject" (Art. 7, Paragraph d)); "legitimate interests pursued by the controller or third party" (Art. 7, Paragraph f))[12]. The same applies to Art. 13 of the Directive (see Section 1.2 below).

The legislative framework that pertains to data protection in Europe has been further enhanced by the adoption of the European Data Retention Directive in 2006.[13] Finally, the right to data protection is also part of the Lisbon Treaty (Art. 16 TFEU).

The subject's right of access to data and its interpretation at European level

The subject's right of access to personal data is enshrined in Art. 12 of the European Data Protection Directive. It imposes on Member States the obligation to guarantee every data subject the ability to obtain from the controller "without constraints at reasonable intervals and without excessive delay or expense":

(a)
- "confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions".

The data subject should be given the possibility to obtain from the controller:

(b) "as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

[11] Art. 8.2 a) and b) of the Directive establish specific exceptions to the prohibition of the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.

[12] Korff, Douwe, *The feasibility of a seamless system of data protection rules for the European Union, Study for the European Commission*, 1998, http://bookshop.europa.eu/en/the-feasibility-of-a-seamless-system-of-data-protection-rules-for-the-european-union-pbC11998407/ (last accessed 5 June 2013). Korff, Douwe, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, Working paper No. 2, Data protection laws in the EU, Study for the European Commission, 2010.

[13] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC of 15 March 2006, OJL 105, 13.04.2006, p. 54-63.

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort".

Hence, although with a veiled expression, Art. 12 entitles the data subject to exercise the following four rights:

1. the right to confirmation as to whether or not data relating to the data subject are being processed by a particular controller and, if so, to obtain details of the processing (Art. 12 (a), first indent);
2. the right of access to one's data, including the right to have a copy of the data in question with any available information as to their source (Art. 12 (a), second indent);
3. the right to have the data rectified, erased or blocked if they do not conform to the Directive, in particular if they are incomplete or inaccurate (Art. 12 (b));
4. the right to be informed about the logic used in case of automated decisions (Art. 12 (a), third indent).

At the time of the adoption of the European Data Protection Directive, the first three rights mentioned here-above did not constitute a novelty. Actually, they were already contained in the OECD Guidelines on data protection[14] and in Convention 108[15]. On the contrary, this was not the case of the right to be informed about automated decisions.

Given the provisions established by Art. 12 of the Directive, it is possible to deduce that the right of access to personal data is a peculiar right which has a two-folded nature and scope. Firstly, it consists of the mere access of the data subject to his personal data. According to the existing legal framework, this right is granted as long as the data controller recognises the entitlement of the data subject to get such access. In more practical terms, the right of access is enacted as long as the data controller accepts the data request of the data subject. Indeed, the true nature of the right of access lays in the concrete entitlement of data subject to make requests to data controllers and find out which of his or her personal data is being processed. Secondly, the right of access to personal data consists in the right of the data subject to have his own data rectified, erased or blocked. It goes without saying that the right of access to personal data can be activated (or rather is enforceable) provided that the data subject can locate the data controller and address him an access request. The dual nature of the right to access to personal data was also emphasised by the ECJ in the case *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*[16] described in Section 1.2.1. The peculiar structure of the right of access to personal data explains why it is often referred to as one of the so-called ARCO rights (right to access, rectification, cancellation, opposition, respectively).

As Gellert and Gutwirth note, the right of access to data is an active right which is exercised through a two-step approach. Firstly, the data subject may ask confirmation as to whether or not his data are being processed. Secondly, in case of positive answer, the data subject has the

[14] As explained in the previous Section, the right of access to data was a corollary of the individual participation principle safeguarded by the OECD guidelines. Ibid.
[15] Art. 8 of Convention 108. Ibid.
[16] ECJ, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, case C-553/07, 7 May 2009.

right to obtain communication of these very data[17]. Although the right of access to personal data is sometimes considered as an ancillary right as compared with the other ARCO rights, it is important to underline that access constitutes the first but irrevocable step towards the full protection of personal data. In other words, it is the *sine qua non* for the exercise of informational rights. In more general terms, a proper protection of the data subjects' rights is not only linked to the exercise of access rights, but also to the obligation of data controllers to notify data subject about the processing of their personal data. Contemplated by Art. 10 and 11 of Directive 95/46/EC, notification has been developed mainly by the Court of Strasbourg as an active duty (from the perspective of the data controller) which guarantees compliance with human rights.[18]

Apart from practical difficulties data subjects can have in getting access to personal data, Directive 95/46/EC mentions specific circumstances in which access rights may be restricted or limited. In particular, Art. 13 entitles Member States to adopt such measures when it is necessary to safeguard interests such as national security (a), defence (b), public security (c), the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions (d), important economic or financial interests (e), certain monitoring, inspection or regulatory functions (f), the protection of the data subject or of the rights and freedoms of others (g). As stressed earlier in Section 1.1, one of the key purposes of the Directive is to reach a sound balance between the protection of personal data and their free movement. The soundness of this exercise is left to a great extent to the interpretation of exceptions to the right to access personal data,[19] established by Art. 13. Concepts such as national security or public security are subject to a broad interpretation and this represents a major problem for the protection of access rights. Moreover, Member States are given great discretion in interpreting those exceptions. As the ECJ underlined in *Lindqvist*, the provisions of Directive 95/46/EC are "necessarily relatively general since it has to be applied to a large number of very different situations".[20] The Directive leaves to Member States the task of deciding the details or choosing between options and their rules contain a degree of flexibility.[21]

In the recent case *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and others*[22] the ECJ underlined that Member States should not invoke exceptions set at Art.

[17] Gellert, Raphaël and Serge Gutwirth, "Citizens access to information: the data subject's rights of access and information: a controllers' perspective", in PRESCIENT, Deliverable 3, *Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data*, 2012, p. 39.

[18] See De Hert, Paul and Franziska Boehm, "The rights of notification after surveillance is over. Ready for Recognition?", in Bus, Jacques, Malcolm Crompton, Mireille Hildebrandt, George Metakides (eds.), *Digital Enlightenment Yearbook 2012*, IOS Press 2012, pp. 19-39.

[19] The exemptions and restrictions provided for in Art. 13 apply also to Art. 6(1), 10, 11 (1), 12 and 21 of the Directive.

[20] ECJ, *Lindqvist*, case C-101/01, 6 November 2003, para. 83. The case concerned Mrs Bodil Linqdvist, a Swedish woman who worked as a catechist in the parish of Alseda (Sweden). She set up internet pages which contained personal data about Mrs Lindqvist herself and eighteen colleagues in the parish, including their names, telephone numbers, the jobs they held, their hobbies and personal and family circumstances. The ECJ ruled that the publication on the internet of those personal data constituted processing of personal data by automatic means within the meaning of Art. 3(1) of Directive 95/46/EC.

[21] Ibid.

[22] ECJ, *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and others*, case C-473/12, 7 November 2013. The Belgian Institute of Estate Agents used private detectives to check whether the activity of Mr Englebert, Immo 9 SPRL and Mr Francotte was in accordance with the proper practice of the profession of real estate agents. IPI found out that Mr Englebert, Immo 9 SPRL and Mr Francotte had acted against these rules

13 for the sole purpose of derogating from obligations descending from the Directive itself. The Court held that Art. 13(1) should not be applied in absolute terms as it provides Member States with the possibility (and not the obligation) to lay down in their national law exceptions to Articles 6 (1), 10, 11 (1), 12 and 21 of the Directive.[23] Moreover, derogating measures may be adopted "only when they are necessary. The requirement that the measures be 'necessary' is thus a precondition for the application of the option granted to Member States by Article 13 (1), and does not mean that they are required to adopt the exceptions at issue in all cases where that condition is satisfied".[24] Although the case *Institut professionnel des agents immobiliers (IPI)* dealt with the application of Art. 10 and 11 (1) of the Directive, the considerations of the Court concern also the right of access (Art. 12). Member States may provide exceptions to the right of access in accordance with Art. 13 (1) of the Directive, provided that it is necessary to introduce such measures. It is for Member States to prove that exceptions they might have introduced were necessary.

Relevant European case law

If we look back at the European case law on data protection and access rights in particular, we find that it has developed in a sort of process of stratification not only of different cases but also of judgments given by different courts. Conventionally, it is possible to identify three distinct periods in the evolution of data protection as a human right, each of which set a milestone in the development of data protection legislation. From 1953 to 1995, the legal basis for the safeguard of data protection rights was represented by the European Convention on Human Rights and its Art. 8, together with the OECD Guidelines and Convention 108. The adoption of Directive 95/46/EC strengthened the legal basis for the protection of personal data (1995-2000). Finally, the European Charter of Fundamental Rights has given data protection an autonomous human right status (2000 onwards). Accordingly, while early judgments were given by the Court of Strasbourg and were based on Art. 8 of the Convention, cases were addressed to the Court of Luxembourg as of the mid-90s. As a consequence, the jurisprudential framework of data protection in Europe appears like a complex and articulated puzzle moving towards an internal coherence. The following paragraph will thus provide an overview of the most relevant case law on access rights at European level.

In the view of the ECtHR, the right of access to personal data is framed in terms of a balance between competing and conflicting interests, according to the principles enshrined in Art. 8.2 ECHR. In *Leander v. Sweden*[25] the applicant, a Swedish citizen working for the Naval Museum in the city of Karlskrona as a technician, started a complaint against the Swedish government. A few days after his appointment, he was told to leave his work pending the outcome of a personnel control which was carried out on him in accordance with the Swedish Personnel Control Ordinance of 1969. Having enquired about the reasons for this decision, he was advised that the control measure had been carried out for security purposes. The contested decision was taken on the basis of information stored on a register maintained by secret security services to which Mr Leander was not given any access. Hence, he asked the Swedish government to have access to those files kept by the Navy and complained that the

---

and asked the Chamber of Commerce of Charleroi to order them to cease their estate agency activities. The ECJ was confronted with the question of whether the direct and indirect processing of personal data of the defendants constituted a violation of Art. 10 and 11(1) of the Directive or was covered by the exception in Art. 13(1)(d). The Court found that this exception applied to the case at stake.

[23] Ibid., para. 32. Indeed, in accordance with the wording of Art. 13 (1), Member States "may" adopt such exceptions.

[24] Ibid.

[25] ECtHR, *Leander v. Sweden*, application no. 9248/81, judgment of 26 March 1987.

government should have made him aware of the information retained about him. The government rejected the whole of the applicant's complaints and as a result, Mr Leander alleged (among other things) a violation of Art. 8 ECHR. The ECtHR assessed that the storing and release of information pertaining to the private life of the applicant amounted to a violation of Art. 8.1 ECHR[26]. However, the Court found that the supposed violation constituted a legitimate interference according to Art. 8.2 ECHR[27]. The Court argued that in the case at stake, the interference "had a valid basis in domestic law" (in accordance with the Personnel Control Ordinance) and that the national legislation was accessible[28]. In addition, it was foreseeable considering that it gave citizens "adequate indication as to the scope and the manner of exercise of the discretion conferred on the responsible authorities to collect, record and release information under the personnel control system".[29] The most interesting arguments of the Court concern certainly the assessment of the requirement of necessity, according to Art. 8.2 ECHR. After having recalled that Member States enjoy a certain margin of appreciation in pursuing national security, the ECtHR stated that it is legitimate for a State to collect and store in registers not accessible to the public secret information and to use such information "when assessing the suitability of candidates for employment in posts of importance for national security"[30]. However, the Court recognised also that in the case at stake (and in matters of national security) the margin of appreciation enjoyed by States was a wide one and that appropriate safeguards were needed accordingly[31]. The Court found them in the procedure set up at national level to the release of information, since a specific Parliamentary Board decided on the disclosure of the information required by the applicant and its composition and functions provided adequate guarantees of neutrality, independence and impartiality[32]. In summary, while the decision of the court went against the individual data subject, the judgement reinforced the importance attached to the presence of an independent and impartial authority as the decision making body in cases where access to data is disputed.

The Court reached a different conclusion in *Gaskin v. UK*.[33] Mr Gaskin was a British citizen who had been in the care of Liverpool City Council in his childhood. At the age of majority, he contended that he was ill-treated in care and sued the local authority for negligence. In the framework of this proceeding he wished to obtain details of where he was kept, by whom and in what conditions. Case records were kept by the Social Services Department of Liverpool City Council and Mr Gaskin addressed a request to this institution to obtain access to the files. Access to the records was denied for reasons of confidence on the grounds that the disclosure of such information would have been contrary to public interest. Further to the appeal judgment, Mr Gaskin alleged a breach of Art. 8 ECHR. The ECtHR recognised that the failure of the applicant to access his case-files fell within the ambit of Art. 8 ECHR given that those documents contained highly personal aspects of his childhood, development and history and thus were part of his "private and family life"[34]. On the one hand, the Court recognised that the confidentiality of the records "contributed to the effective operation of the child-care

[26] ECtHR, *Leander v. Sweden*, para 48.
[27] Ibid., para 67.
[28] Ibid., para 52-53.
[29] Ibid., para 56.
[30] Ibid., para 59.
[31] Ibid., para 59-63.
[32] Each of the members of the board had a right of veto. Furthermore, a Parliamentary Committee on Justice scrutinised the decisions of the Board and the Parliamentary Ombudsman supervised its activity. ECtHR, *Leander v. Sweden*, para 65-66.
[33] ECtHR, *Gaskin v. the United Kingdom*, application no. 10454/83, judgment of 7 July 1989.
[34] ECtHR, *Gaskin v. the United Kingdom*, para 36-37.

system" and served a legitimate aim, according to the rules set forth in the Local Authority Circular of 1983[35]. On the other, it stressed the fact that in the present case the applicant had a "vital interest, protected by the Convention, in receiving the information necessary to know and to understand" information concerning his past life[36]. Hence, the Court struck a fair balance between these two competing interests while looking at the internal procedure established by the City Council to allow access to personal records. Ultimately the ECtHR found that the system for granting access was not in accordance with the principle of proportionality as there was no independent authority who decided on the access requests[37]. Thus, in the *Gaskin* case the judgement found that the City Council had not adequately balanced the data subject's right of access against other consideration and as such, this constituted a disproportionate interference with Mr Gaskin's right of access.

Similar findings were reached in the case *M.G. v. UK*[38]. Like in *Gaskin*, the case concerned a British citizen who had been in voluntary care with the Social Services Department of the local authority for five periods when he was a child. His mother had mental health problems while his father had some difficulties coping with children. Having been abused as a child, in 1995 Mr M.G. requested access to social service records. In particular, he was looking for information as to whether he had ever been on a "risk register", whether his father had ever been convicted of crimes against children and about the responsibility of the local authority for abuses he had suffered. The local authority provided the applicant with information about his childhood in several occasions. However the applicant complained about the fact that authorities never gave him full access to his file. Like Mr Gaskin, Mr M.G. claimed that his right to private and family life had been infringed (on the basis of Art. 8 ECHR) because of the unimpeded access to all social service records relating to him. The Court shared the applicant's view and considered also that he could not rely on his parents as a "satisfactory source of information"[39]. When addressing the issue of proportionality, the ECtHR pointed out that the decision about denial of access, as in the *Gaskin* case, had not been taken by any independent authority. Moreover, because of this the applicant was not given the possibility to challenge the refusal of access[40]. Hence, the Court concluded that the denial of access to social service records resulted in the failure of the UK government to "fulfil the positive obligation to protect the applicant's private and family life"[41].

All of the cases mentioned above illustrate that in the ECtHR's view, an access denial is disproportionate (and thus illegitimate) under Art. 8 ECHR if the concerned decision does not strike a fair balance between competing interests and, in particular, has not been taken by an independent and impartial authority. Although the Court emphasises the role of such authority, it is important to note that proportionality refers broadly to the way in which those interests are struck at national level through national legislation. The Court stressed this aspect in *Odièvre v. France*[42]. The case concerned a French national who had been abandoned by her natural mother at birth. Her mother requested that her birth be kept secret and her identity confidential. The applicant was placed with the Social Services Department and then adopted when she was four. Later on, the applicant requested access to information about her birth and permission to obtain copies of any documents which could reveal facts about her natural

[35] Ibid., para 43.
[36] Ibid., para 49.
[37] Ibid.
[38] ECtHR, *M.G. v. the United Kingdom*, application no. 39393/98, judgment of 24/12/2002.
[39] Ibid., para 28-29.
[40] Ibid., para 30.
[41] Ibid., para 31.
[42] ECtHR, *Odièvre v. France*, application no. 42326/98, judgment of 13 February 2003.

family. The Social Services Department rejected her request and hence she started a legal proceeding which eventually came before the ECtHR. In considering the admissibility of the case, the Court stated that "birth, and in particular the circumstances in which a child is born, forms part of a child's, and subsequently the adult's, private life guaranteed by Article 8 of the Convention"[43]. It further recognised that the right to know one's origins derives from a wide interpretation of private life[44]. The Court made clear that unlike the *Gaskin* case, the applicant's aim in the present case was not to know about her past life and childhood, but to "trace another person, her natural mother" who had expressly requested that "information about the birth remain confidential"[45]. Hence, the ECtHR balanced the applicant's right to know about her origins with her mother's interest in remaining anonymous. The Court considered that the French law of 22 January 2002 on access by adopted persons and people in State care to information about their origins gave the applicant the possibility to search for information about her biological origins. An independent and impartial council had been established at national level to handle access requests and so the applicant had the possibility to know about her mother's identity. On the basis of these considerations the Court found that national legislation reconciled both interests at stake and no violation of Art. 8 ECHR had occurred.

The most remarkable judgment of the ECJ on access rights is certainly *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*[46]. The case originated in a proceeding between Mr Rijkeboer and the Board of Aldermen of Rotterdam (hereafter 'the College') concerning the partial refusal of the College to grant Mr Rijkeboer access to information on the recipients of personal data relating to him during the period of one year preceding his request for access. Mr Rijkeboer requested that the College notify him of all circumstances in which data relating to him had been disclosed to third parties in the two years preceding his request. The College replied to his request providing him with the details of the recipients to whom data had been disclosed, but to the period of one year preceding his request, in accordance with national legislation[47]. Following the judge of appeal's referral of the case to the ECJ, it was necessary to establish whether Art. 12 of Directive 95/46/EC were compatible with a national provision which set the time limit of one year to the exercise of the individual's right of access to information on the recipients or categories of recipient of personal data. Firstly, the Court made clear the role of Art. 12 of the Directive in the framework of data protection legislation. It stated that the right of access to personal data is necessary to enable the data subject to exercise the right to rectify, erase or block his personal data or to notify this to third parties. Moreover, as the Court pointed out, the right of access is also necessary to enable the data subject to exercise his right to object to the processing of personal data[48]. In order to exercise these two different categories of rights, data access "must of necessity relate to the past"[49]. Secondly, in the present case the Court balanced the right of the data subject (and of the rights descending from it) with the burden of the data controller to store personal data. Indeed, as the Court noted, the legal obligation to keep the data subject's personal data for a long period of time would represent for the data controller a disproportionate effort under the terms of the Directive. Member States' legislation should

[43] ECtHR, *Odièvre v. France*, para 29.
[44] Ibid., para 44.
[45] Ibid., para 43.
[46] ECJ, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, case C-553/07, 7 May 2009.
[47] Indeed, Art. 103 (1) of the 1994 Law on personal data held by local authorities established that information on the recipients had to be kept by the College for one year only.
[48] ECJ, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, para 51-52.
[49] Ibid., para 54.

strike a fair balance between the data subject's and the data controller's interests and national courts should make the verifications necessary to assess the fairness of such balance. In the *College van burgemeester* case, the Court assessed that the right of access to personal data does not only refer to the present, but also to the past. It follows that that the rule limiting the storage of information on the recipients or categories of recipients to a period of one year does not constitute "a fair balance of the interest and obligation at issue", unless it could be proved that longer storage would represent an excessive burden on the data controller[50]. The balance of the data controller's and data subject's conflicting interests made by the ECJ in the *College van burgemeester* case is in line with the main principles and aims of Directive 95/46/EC.

The European case law we examined in this Section tell us that European courts have developed different attitudes towards the operationalization of access rights. The Court of Strasbourg considers the right of access to personal data in a holistic way, in which access needs to be balanced against other fundamental rights and interests. Indeed, balance is the common denominator in all cases of the ECtHR described above. When Member States strike a fair balance between rights or interests which may come into conflict and establish certain procedures to allow data subjects to exercise access rights, no violation occurs. In particular, the judgment of the Court on the proportionality principle hinges upon the existence of an independent, neutral and impartial authority at national level which handles data access requests. According to the Court, this is the only requirement on the basis of which national provisions or decisions need to be tested, irrespective of whether or not access is granted. As a consequence, the right of access is violated when that independent authority is not established at national level (like in *Gaskin*). In other cases, although access is denied, there is no violation of access rights when such independent authority is set up (like in *Leander* and *Odièvre*). These reflections lead us to the conclusion that the Court of Strasbourg does not consider access rights in absolute terms and provides a protection that is more relative than what data protection norms would push for.

Although the Court of Luxembourg has rarely ruled on access rights, its emphasis has been on the compliance of national law with the provisions of Directive 95/4C/EC, so interpreting its norms. The need to balance conflicting interests is also present in the case law of the ECJ, but with a special focus on the data subject and the data controller. So far the Court has interpreted Art. 12 of the Directive in a rather extensive way, referring the right of access to personal data also to the past (*College van burgemeester* case) and accepting limitations to this right only when necessary (see the case *Institut professionnel des agents immobiliers (IPI)*, analysed above). The 'revival' of access rights in the proposed data protection reform (see further below) may confirm this orientation in the future.

Finally, it is worth mentioning the ECJ's judgement in May 2014 in a case brought by the Spanish DPA against Google. Although the case did not concern access rights specifically, the court's finding is likely to have a wide ranging impact on data subjects' management of their personal data. The case concerned a Spanish citizens' request to Google that they remove a link which appeared when one searched for the citizen's name using the corporation's search engine. The result in question related to a historical matters pertaining to the citizen's financial problems. Having failed to obtain a resolution with Google, the Spanish DPA (the AEPD), brought proceedings before the ECJ. The court ruled that Google was indeed responsible for removing results from its search engine in certain cases despite the fact that

[50] Ibid., para 66.

the content itself was managed by third parties[51]. The judgement appeared to underscore the so-called 'right to be forgotten' insofar as allowing data subjects to request that information about their past is deleted from search engine results in cases where 'the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed'[52].

The promotion of access rights by the EDPS and European authorities and their role in ensuring compliance to European norms

The European Data Protection Supervisor (EDPS) was established in 2001 with Regulation 45/2001.[53] The EDPS is the independent supervisory authority responsible for monitoring all data processing operations carried out by Community institutions or bodies (Art. 1). This institution is responsible for supervising and ensuring the application of Regulation 45/2001, as well as of Community law relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body. Nonetheless, the EDPS advises Community institutions and bodies and data subjects on "all matters concerning the processing of personal data" (Art. 41, Paragraph 2). Its appointment, powers, duties, staff and financial resources and guarantees of independence are laid down in Art. 41-49 of the Regulation. In particular, the EDPS (Art. 46):

- hears and investigates complaints, and inform the data subject of the outcome within a reasonable period;
- conducts inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;
- monitors and ensures the application of the provisions of this Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body;
- advises all Community institutions and bodies on all matters concerning the processing of personal data;
- monitors relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;
- cooperates with national DPAs;
- participates in the activities of the Article 29 Working Party (see infra).

Furthermore, the EDPS may order the rectification, blocking, erasure or destruction of data processed against the provisions of Regulation 45/2001, impose a ban on the processing, intervene in judicial actions before the Court of Justice or defer matters to other European institutions (Art. 47).

The EDPS is more than a mere controlling body. As it has been pointed out, over the time it has contributed to shape European data protection policies and to develop data protection

[51] See full judgement of Case C-131/12 available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=260714#Footnote*

[52] Press release from Case C-131/12 available at http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

[53] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001, L 8/01.

legislation.[54] The position of the EDPS in the area of data subject's rights is enshrined in Opinions on data processing and in its recent "Guidelines on the rights of individuals with regard to the processing of personal data".[55] With the objective to promote a data protection culture in Europe, the Guidelines are addressed to "all services within the EU administration that process personal data".[56] In the words of the EDPS, the right of access to personal data consists in the right to receive from the data controller, notably an EU institution, "information as to whether or not personal data relating to them are being processed, as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed as well as communication in an intelligible form of the personal data undergoing processing".[57] Recalling Art. 13 of Regulation 45/2001,[58] the EDPS' guidelines state that the right of access can be exercised at any time, free of charge and information has to be disclosed within three months from the receipt of the request. Although the EDPS guidelines do not apply to the processing of personal data performed by organisations other than EU institutions, they represent a useful tool to interpret legal provisions and raise awareness over access rights and data protection.

For the purposes of this research it is also important to notice that the EDPS issued specific guidelines on video-surveillance in 2010 which are addressed to European Union institutions operating video-surveillance equipment.[59] Although these guidelines do not focus specifically on the right of access of data subjects to CCTV footage, they contain useful provisions about whether to use video-surveillance, how to secure personal information and how to ensure accountability. Specific guidelines are given as regards the on-the-spot pictogram which informs individuals about the operation of a CCTV camera. According to the EDPS, the pictogram should:

- identify the 'controller' (the name of the Institution is usually sufficient);
- specify the purpose of the surveillance ("for your safety and security" is usually sufficient);
- clearly mention if the images are recorded;
- provide contact information and a link to the on-line video-surveillance policy.[60]

Moreover, if an area outside a building is under surveillance, this should be clearly stated. However, if an area is under surveillance it is not necessary and several cameras are installed therein, it is not necessary to put a notice next to every single camera.

---

[54] De Hert, Paul and Papakonstantinou Vagelis, "The EDPS as a unique stakeholder in the European data protection landscape, fulfilling the explicit and non-explicit expectations", in Hijmans, Hielke and Herke Kranenborg (eds.), *Data Protection Anno 2014: How to Restore Trust?, Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*, Intersentia, pp. 237 - 252.

[55] EDPS, "Guidelines on the rights of individuals with regard to the processing of personal data", 25 February 2014, pp. 1-40, p. 7.

[56] See the EDPS press release, EDPS, "EDPS Guidelines on the rights of individuals: data protection is essential to good public administration", 25 February 2014, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/EDPS-2014-05-Guidelines_DS_rights_EN.pdf (last accessed 20 March 2014).

[57] Ibid.

[58] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Official Journal of the European Communities, 12 January 2001.

[59] EDPS, "The EDPS video-surveillance guidelines", 17 March 2010, pp. 1-64.

[60] Ibid., p. 43.

According to the EDPS' video-surveillance guidelines if a data subject submits an access request claiming access to CCTV images kept by EU institutions, his/her request should be answered within 15 calendar days. If specific access requests are introduced, EU bodies should grant access to the images "by allowing the individual to view the recordings or by providing a copy to him/her".[61] As pointed out earlier with regards to the EDPS guidelines on the processing of personal data, although these provisions on video-recordings apply only to CCTV cameras installed by European institutions, they can be considered as best practices in the use of such devices.

Art. 28 of Directive 95/46/EC establishes national Data Protection Authorities (DPA). They are intended to be responsible for monitoring the application of the provisions of the Directive at national level and act with complete independence in the exercise of their functions. In particular, they are endowed with:

- investigative powers and powers to collect all information necessary for the performance of its supervisory duties;
- power of intervention that can be exercised either by delivering opinions or ordering the blocking, erasure or destruction of data, or imposing a ban on processing, or warning or admonishing the data controller, or referring the matter to political institutions;
- the power to engage in legal proceedings or to bring violations before judicial authorities.

Accordingly, national DPAs act like judicial authorities of first instance in the framework of a trial, in case of data protection violations. Their decisions are then subject to appeal before national courts. This implies that national DPAs "shall hear claims lodged by any person, or by an association representing that person" (Art. 28, Paragraph 4).

In addition to national DPAs, the Data Protection Directive sets up the Article 29 Data Protection Working Party (DPWP) (Art. 29-30). It is an advisory body that acts independently. It promotes the uniform application of Directive 95/46/EC cooperating with national DPAs. In addition, the DPWP issues recommendations to EU institutions and the public on data protection matters and gives opinions on codes of conduct adopted at European level.

Thus, from the perspective of data subjects, DPAs can be considered as the first institutions engaged in ensuring the enforcement of data protection laws. As pointed out by the European Union Agency for Fundamental Rights (FRA), the possibility for individuals to invoke data protection violations is a corollary of the right to an effective remedy which descends from Art. 47 (1) of the European Charter of Fundamental Rights and Art. 13 of the ECHR.[62] How do DPAs operate to enforce the subject's right of access to data? Do they do so? Are they willing or capable to do so? It is not possible to answer these questions univocally. Practices are very different and articulated in EC and EEA states and these differences are also dependent upon the specific legislations in place at national level. Moreover, it is often hard to undertake such analysis especially in those Member States that joined the Union in the last

[61] Ibid., p. 45.
[62] FRA, *Access to data protection remedies in EU Member States*, European Union Agency for Fundamental Rights, 2013, pp. 1-59.

decade.[63] The individual country reports that are part of this study will map and highlight those differences at national level.

Doubts about the way data protection legislation is enforced within the European Community were expressed by the ECJ in the case *Commission v. Germany*[64]. The case originated from a dispute between the Commission (supported by the EDPS) and Germany about the interpretation of the words "with complete independence" of Art. 28.1 of Directive 95/46/EC. According to the German law, the activity of regional DPAs (authorities established at the Länder level) was expressly subjected to State scrutiny. The Commission argued that this scrutiny was against the requirement of complete independence of DPAs and so constituted an infringement of Directive 95/46/EC. In particular, the Commission relied on a broad interpretation of the contested provision and claimed that DPAs had to be free from any influence no matter if that that influence was exercised within or outside the public administration. By contrast, Germany opposed that interpretation holding that the requirement of independence implied that DPAs had to be free from external influences only, that is influences exercised by non-public bodies. Accordingly, Germany considered the State scrutiny exercised in the Länder simply as an "administration's internal monitoring mechanism". [65] The Court shared the Commission's views and embraced a broad interpretation of Art. 28.1 of the Directive. It pointed out that "when carrying out their duties, the supervisory authorities must act objectively and impartially. For that purpose, they must remain free from any external influence, including the direct or indirect influence of the State or the *Länder*."[66] Moreover, the Court stated that the requirement of independence precludes any external influence, whether direct or indirect, which could call into question the performance by DPAs of their tasks and competences descending from the Directive.[67] Hence, the Court recognised that the State scrutiny exercised over regional DPAs was not consistent with the requirement of independence of Art. 28.1 of the Directive.[68] Taking into account the considerations of the ECJ in the case *Commission v. Germany*, we can say that the more problematic aspects concerning the role of national DPAs are the following: election and independence, functions and level of engagement and collaboration among DPAs.[69] These aspects will emerge more clearly in Section 2 of this Deliverable.

The right of access to data and the European data protection reform

In 2012 the European Commission proposed a new legal framework to regulate data protection in Europe[70]. The data protection reform was exacerbated by the need to provide answers to key questions emerging in the information society and in particular to:

[63] Indeed, it is quite difficult to understand whether and to what extent DPAs from Eastern European countries are involved in promoting access rights. This is partly due to the fact that these Member States joined the EU ten years ago and since then made efforts to implement Directive 95/46/EC.
[64] ECJ, *European Commission v. Federal Republic of Germany*, case C-518/07, 9 March 2010.
[65] ECJ, *European Commission v. Federal Republic of Germany*, para 16.
[66] Ibid., para 25.
[67] Ibid., para 30.
[68] Ibid., para 37.
[69] Ibid., para 24-25 and 30.
[70] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, Brussels, 25 January 2012. European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigations, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (General Data Protection Directive), COM(2012) 10 final, Brussels, 25 January 2012.

- new technological changes and challenges;
- exponential growth of digital information and communication;
- the internationalisation of exchange of personal data;
- the use of commercial data for law enforcement purposes[71].

The proposed data protection reform prescribes more supervision and enforcement of data protection norms by national DPAs and measures to enhance the subject's control over personal data. This entails strengthening rights, introducing a right to object to profiling, clarifying the concept of consent, enhancing transparency, rights to data portability, making more effective the exercise of rights and the deletion of unnecessary data. Although a detailed analysis of the provisions of the new Regulation and Directive would fall out of the scope of this report, it is necessary to make reference to some of the new provisions that should have a significant impact on the access rights. As mentioned, the reform stresses the role of consent in the relationship between the data subject and the data controller. The new Art. 7 of the Regulation safeguards the right of the data subject to withdraw his/her consent to the processing of personal data at any time and establishes that consent shall not provide a legal basis for the processing when there is a significant imbalance between the controller and the data subject. Art. 11 would introduce on data controllers the obligation to provide transparent, easy accessible and understandable information to the data subject. Building on Art. 12 of Directive 95/46/EC, Art. 15 of the Regulation would strengthen the right of access to personal data. Among other things, it would impose on the data controller the obligation to inform the data subject about the storage period of the personal data, the rights to rectification and erasure and how to lodge a complaint.

The proposed Directive devotes its chapter III to the rights of the data subject. According to Art. 10, Member States shall provide that the controller takes appropriate steps to have transparent and easily accessible policies for the exercise of data subject's rights. Information and communication about data processing in criminal matters shall be given by the data controller to the data subject in an intelligible form, in clear and plain language. Data access shall be exercised free of charge and follow-up to access rights requests shall be provided "without undue delay".[72] Articles 11 and 12 of the Directive mention all information the data controller has to provide the data subject in case personal data are collected from the data subject himself or from a third person (i.e. the purpose of the processing, the recipients or categories of recipients to whom personal data have been disclosed, the storage period, etc.). This obligation to inform may be restricted if information may obstruct inquiries, investigations or procedures, or cause prejudice to the prevention, detection, investigation and prosecution of crime. Exceptions of this kind apply also when public security, national security and the rights and freedoms of others are at stake. In cases where direct access is restricted, data subjects shall be given the possibility to exercise indirect access (Art. 14).

Thus, the overall legal framework of the new proposal goes in the direction of giving data subjects more powers in order to challenge data protection infringements. However, despite

[71] Hielke Hijmans, "Recent developments in data protection at European Union level", *ERA Forum*, Vol. 11, Issue, 2, Springer, 2010, pp. 219-231, p. 223.

[72] However, if a request has a vexatious character a fee may be charged.The new Directive underlines that in this case the controller has the burden of proving that the concerned request is vexatious.

the efforts to improve Directive 95/46/EC, the data protection reform does not prevent legal uncertainties and a certain scepticism as to the practical consequences it will entail[73].

Conclusion

The right of access to personal data constitutes a peculiar right in the framework of the European data protection legislation. Its legitimation descends from Art. 12 of Directive 95/46/EC whose constitutional roots lay partly in the European Convention on Human Rights and partly in the more recent Charter of Fundamental Rights of the European Union. Like data protection, data access does not have a long tradition as a European fundamental right and this is reflected in the limited case law in this area. Indeed, the case law presented in this report illustrates some of the main obstacles that prevent the right of access to personal data to be fully enforceable. The lack of information regarding the duration of the storage period of personal data and the lack of an independent authority that arbitrates on access requests represent two examples of such obstacles.

The European case law on access rights stresses the need to set a fair balance (or provide a mechanism via which to strike this balance) between the data subject's and the data controller's interests. Nonetheless, European Courts require that balance to be reached at national level. Although the proposed data protection reform represents an attempt to set that balance at European level, there is still a long way to go before implementing the right of access to personal data across Europe. However, given the scale of today's surveillance and the data protection concerns stemming from it, it is reasonable to believe that European citizens will become more familiar with access rights and access requests in the future and that this right will thus develop further from theory to practice.

References

Legislation and case law

Charter of Fundamental Rights of the European Union, *Official Journal of the European Union* C 83, 30.3.2010, 389-403.

Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, 1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (last accessed 5 June 2013).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

ECJ, *Lindqvist*, case C-101/01, 6 November 2003.

ECJ, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, case C-553/07, 7 May 2009.

ECJ, *European Commission v. Federal Republic of Germany*, case C-518/07, 9 March 2010.

[73] Paul De Hert, Vagelis Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, Vol. 28, 2012, pp. 130-142.

ECJ, *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and others,* case C-473/12, 7 November 2013.

ECtHR, *Gaskin v. the United Kingdom*, application no. 10454/83, judgment of 7 July 1989.

ECtHR, *Leander v. Sweden*, application no. 9248/81, judgment of 26 March 1987.

ECtHR, *M.G. v. the United Kingdom*, application no. 39393/98, judgment of 24/12/2002.

ECtHR, *Odièvre v. France*, application no. 42326/98, judgment of 13 February 2003.

European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigations, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (General Data Protection Directive), COM(2012) 10 final, Brussels, 25 January 2012.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, Brussels, 25 January 2012.

OECD Recommendation concerning Guidelines governing the protection of privacy and transborder flows of personal data of 23 September 1980.

Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001, L 8/01.

Literature

Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13 July 2011, p. 2.

De Hert, Paul and Papakonstantinou Vagelis, "The EDPS as a unique stakeholder in the European data protection landscape, fulfilling the explicit and non-explicit expectations", in Hijmans, Hielke and Herke Kranenborg (eds.), *Data Protection Anno 2014: How to Restore Trust?, Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*, Intersentia, pp. 237 - 252.

De Hert, Paul and Vagelis Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, Vol. 28, 2012.

De Hert, Paul and Franziska Boehm, "The rights of notification after surveillance is over. Ready for Recognition?", in Bus, Jacques, Malcolm Crompton, Mireille Hildebrandt, George Metakides (eds.), *Digital Enlightenment Yearbook 2012*, IOS Press 2012, pp. 19-39.

Dinan, Desmond, Ever Closer Union? An introduction to European integration, Basingstoke, Palgrave Macmillan, 2010.

EDPS, Legitimate reasons for processing of personal data, https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA6 (last accessed 7 January 2014).

EDPS, "Guidelines on the rights of individuals with regard to the processing of personal data", 25 February 2014, pp. 1-40.

EDPS, "EDPS Guidelines on the rights of individuals: data protection is essential to good public administration", 25 February 2014, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/EDPS-2014-05-Guidelines_DS_rights_EN.pdf (last accessed 20 March 2014).

EDPS, "The EDPS video-surveillance guidelines", 17 March 2010, pp. 1-64.

FRA, *Access to data protection remedies in EU Member States*, European Union Agency for Fundamental Rights, 2013, pp. 1-59.

FRA, *Data protecction in the European Union. The role of national data protection authorities. Strengthening the fundamental rights architecture in the EU II*, European Union Agency for Fundamental Rights, 2010, pp. 1-50.

Fuster, Gloria Gonzales and Raphaël Gellert, "The fundamental right of data protection in the European Union: in search of an uncharted right", *Review of Law, Computers & Technology*, Vol. 26, No. 1, 2012.

Gellert Raphaël, and Serge Gutwirth, "Citizens access to information: the data subject's rights of access and information: a controllers' perspective", in PRESCIENT, Deliverable 3, *Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data*, 2012.

Hijmans, Hielke, "Recent developments in data protection at European Union level", *ERA Forum*, Vol. 11, Issue, 2, Springer, 2010.

Korff, Douwe, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, Working paper No. 2, Data protection laws in the EU, Study for the European Commission, 2010.

Korff, Douwe, *The feasibility of a seamless system of data protection rules for the European Union, Study for the European Commission*, 1998, http://bookshop.europa.eu/en/the-feasibility-of-a-seamless-system-of-data-protection-rules-for-the-european-union-pbC11998407/ (last accessed 5 June 2013).

Rosamond, Ben, *Theories of European integration*, Hampshire: Palgrave, 2000.