This is a draft version. Final version is published in The Computer Law & Security Review, 2015-1.

Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system

B. van der Sloot[1]

Institute for Information Law (IViR), University of Amsterdam, Netherlands

ABSTRACT

Privacy and data protection rules are usually said to protect the individual against intrusive governments and nosy companies. These rights guarantee the individual's freedom, personal autonomy and human dignity, among others. More and more, however, legal persons are also allowed to invoke the rights to privacy and data protection. Prima facie, it seems difficult to reconcile this trend with the standard interpretation of those rights, as legal persons do not enjoy freedom, personal autonomy or human dignity and it seems uncertain why business interests should be protected under privacy and data protection rules. On second thoughts, however, it appears rather unproblematic to grant legal persons partial protection under these regimes, especially when it recognises general duties of care for data processers and governmental agencies.

Keywords: privacy; data protection; legal persons; societal interests; individual interests

1. Introduction

Increasingly, legal persons are invoking rights to privacy and data protection to protect their own interests and that of others. Businesses, for example, claim that their privacy has been violated by governments wire-tapping their communication systems or confiscating business documents. Companies, such as internet providers who groan under data retention and other obligations, point not only to their own interests, but also to their position being intrinsically connected to the (privacy) concerns of their users. The National Security Agency (NSA)- Edward Snowden affair has added to such assertions, for example by Google, Facebook and others, who have called on the American government to protect the interests of the American citizen and stop monitoring their communication channels.[2] In similar fashion, together with a natural person, three limited companies have issued a complaint before the European Court of Human Rights (ECtHR) in a class action, relying on the general interests to stop illegal mass surveillance practices by the British government.[3]

[1] Bart van der Sloot, Institute for Information Law (IViR), University of Amsterdam, Postbus 1030 1000 BA Amsterdam Netherlands. Email address: b.vandersloot@uva.nl

[2] <https://www.reformgovernmentsurveillance.com/>.

[3] <https://www.privacynotprism.org.uk/assets/files/privacynotprism/letter_from_ecthr_to_uk_gov.pdf>.

But can legal persons invoke privacy and data protection legislation and should they be allowed to? Traditionally, privacy and data protection are only granted to natural persons. Legal institutions usually do not play a central role in the enjoyment of the right to privacy, such as for example a church may do with respect to the right to freedom of religion or a press agency in relation to certain forms of the freedom of expression.[4] Moreover, privacy is usually related to individual interests,[5] such as dignity,[6] autonomy[7] or freedom, either negative liberty[8] or positive liberty,[9] and not to societal interests. This in contrast with rights such as the freedom of expression, which (at least partially) protects the societal interest related to the general search for truth through the market place of ideas and the well-functioning of a free press as a necessary precondition of every free and democratic state. Consequently, class actions are often declared inadmissible if related to privacy or data protection claims.[10] In the standard approach, the applicant of a privacy claim should be a natural person who seeks protection for his individual interests. As more and more legal persons are also allowed to invoke the right to privacy and the related right to data protection, the question becomes whether this traditional focus still holds.[11]

This article describes in how far legal persons can and should be able to rely on the rights to privacy and data protection. This question has a descriptive element, namely to what extent legal persons, under the current paradigm, can rely on the protection granted by these doctrines. The question also has a normative element, namely in how far legal persons should be able to rely on data protection and privacy instruments to protect their interests. The first element is discussed in sections 2 and 3, the second element in section 4. This study first analyses the material scope of the right to privacy (section 2.1), describes in how far legal persons are allowed to invoke this right (section 2.2) and to what extent their interests are protected (section 2.3). Similarly, the material scope of the right to data protection will be analyzed (section 3.1), it will be described whether legal persons are allowed to invoke data protection provisions (section 3.2) and to what extent they enjoy protection similar to natural persons (section 3.3). The analysis (section 4) will make an effort to describe the fundaments of both rights and analyze in how far they would conflict with granting legal persons and their interest (partial) protection.

[4] See in general: J. D. van der Vyver & J. Witte (eds.), 'Religious human rights in global perspective', The Hague, Nijhoff, 1996. E. Barendt, 'Freedom of speech', Oxford, Oxford University Press, 2007. Council of Europe, 'Freedom of expression in Europe: case-law concerning article 10 of the European Convention on Human Rights', Strasbourg, Council of Europe Publishing, 2007.

[5] Inness focusses on intimacy: J. C. Inness, 'Privacy Intimacy and isolation', New York, Oxford University Press, 1992.

[6] See among others: S. I. Benn, 'Privacy, Freedom, and Respect for Persons'. In: F. Schoeman (ed.), 'Philosophical Dimensions of Privacy: an Anthology', Cambridge, Cambridge University Press, 1984. J. Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty', The Yale Law Journal, 2004, 113.

[7] See among others: B. Roessler, 'The value of privacy', Cambridge, Polity Press, 2005. A. F. Westin, 'Privacy and Freedom', London, The Bodley Head, 1970.

[8] See among others: J. S. Mill, 'On liberty', Norton, New York, 1975. W. von Humboldt, 'The limits of state action', London, Cambridge University Press, 1969.

[9] The classic example is: *Roe v. Wade*, 410 U.S. 113 (1973).

[10] T. Zwart, 'The admissibility of human rights petitions: the case law of the European Commission of Human Rights and the Human Rights Committee', Dordrecht, Nijhoff, 1994.

[11] Some authors have also connected the value of privacy to a defense of a vital democracy. See among others: J. Habermas, 'Between facts and norms', Cambridge, MIT Press, 1996. P. M. Schwartz & W. M. Treanor, 'The new privacy, Michigan Law Review, 101 (2003) 216. J. E. Flemming, 'Securing Deliberative Autonomy, Stanford Law Review, 48 (1995) 1.

Both with regard to the right to privacy and the right to data protection, this contribution will distinguish between four situations. First, the situation in which a legal person represents a natural person in an official complaint. Second, the possibility of bringing forth a complaint on behalf of the general public or the society – the class action. Third, the situation in which the interests of a legal person are part and parcel of the interests of a natural person. Fourth and finally, the situation in which a legal person can bring forth a complaint to protect its own interests.

Four points will be made in this contribution. First, sections 2.1 and 3.1 will make clear that the material scope of both the right to privacy and the right to data protection has extended quite considerably. Both doctrines have their background in laying down rules of good governance and safeguards against the abuse of power. Consequently, they are primarily aimed at protecting societal interests. Both, originally, only marginally provided subjective rights to natural persons. However, both doctrines have undergone a significant change. More emphasis has been placed on the protection of natural persons and their private interests, among others, by giving them a number of subjective rights. Consequently, these instruments now explicitly protect individual interests. Second, sections 2.2 and 3.2 will argue that, although initial definitions allowed for a broad application, in the dominant interpretation, only natural persons have been granted protection under the scope of the right to privacy and the right to data protection. However, in more recent years, both doctrines have been extended to legal persons. Third, sections 2.3 and 3.3 will point out that, even though legal persons can rely on privacy and data protection rules, they are usually only granted partial protection. Fourth and finally, section 4 will argue that both under the right to privacy and under the right to data protection, legal persons should be allowed partial protection. A separation should be made between the protection of societal interest, e.g. safeguards against abuse of power and unlawful data processing, which should also apply to legal persons, and the protection of individual interests, e.g. a right to human flourishing and the right to be forgotten, which should only apply to natural persons.

Two things are important to point out from the start. First, there are differences between the right to privacy and the right to data protection, which will be described in more detail below. Perhaps the most prominent example is the material scope. The right to privacy usually does not extend to the collection of non-private and non-privacy-sensitive data,[12] while the term 'personal data', central to most data protection documents, is not limited to private or sensitive information, but extents to any data with which someone could potentially be identified. 'Even ancillary information, such as "the man wearing a black suit" may identify someone out of the passers-by standing at a traffic light.'[13]

Second, this study will primarily discuss the European perspective and doing so will refer to documents of both the European Union (EU) and the Council of Europe (CoE). For privacy, the case law on Article 8 European Convention on Human Rights (ECHR) will be central to the discussion and with regard to data protection, the EU's Data Protection

[12] J. Kokott & C. Sobotta, 'The Distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR'. In: H. Hijmans & H. Kranenborg (eds.), 'Data Protection anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)', Cambridge, Intersentia, 2014. See in the same book also: C. Docksey, 'The European Court of Justice and the Decade of surveillance'. In: H. Hijmans & H. Kranenborg (eds.), 'Data Protection anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)',

[13] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data', 01248/07/EN, WP 136, 20 June 2007, Brussels, p. 13.

Directive[14] and the Regulation,[15] which will replace the Directive over time, will function as the primary (though not exclusive) points of reference. Still it has to be stressed that the Directive is to a large extent inspired by the CoE's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[16] and that the ECtHR often refers to the EU's Charter of Fundamental Rights when delivering its decision.[17] Consequently, more and more, the instruments of both organizations are intertwined and interrelated and can (and perhaps need to) be studied in connection to each other.

2. The right to privacy

2.1 The scope of the right to privacy

The European Convention on Human Rights was adopted in 1950 and in many respects arises from the ashes of the Second World War.[18] It 'is a product of the period shortly after the Second World War, when the issue of international protection of human rights attracted a great deal of attention. These rights had been crushed by the atrocities of National Socialism, and the guarantee of their protection at the national level had proved completely inadequate.'[19] Like the Universal Declaration on Human Rights, to which the European Convention makes explicit reference in its preamble[20] and on which it is based to a large extent,[21] the Convention is primarily concerned with curtailing the powers of totalitarian states and fascist regimes. Not surprisingly, the *travaux préparatoires* of both documents, reflecting the discussions of the authors of both texts, are full of references to the atrocities of the holocaust and the other horrors of the past decades.

Consequently, the main concern of both the Declaration and the Convention is to protect individuals from the arbitrary interference with their rights and freedoms by intrusive governments. This rationale is even more prominent in the Convention than in the Declaration, because the former document only embodies so called 'first generation' human

[14] 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.
[15] 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), {SEC(2012) 72 final}, Brussels, 25 January 2012, COM(2012) 11 final, 2012/0011 (COD).
[16] <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.
[17] See for example: ECtHR, *Christine Goodwin v. the United Kingdom*, appl.no. 28957/95, 11 July 2002. ECtHR, *I. v. the United Kingdom*, appl.no. 25680/94, 11 July 2002. See further: <http://hub.coe.int/what-we-do/human-rights/eu-accession-to-the-convention>.
[18] G. L. Weil, 'The European Convention on Human Rights: background, development and prospects', Leyden, Sijthoff, 1963.
[19] L. Zwaak, 'General survey of the European Convention', p. 3. In: P. van Dijk et al. (eds.), 'Theory and practice of the European Convention on Human Rights', Antwerpen, Intersentia, 2006.
[20] It specifies: "Considering the Universal Declaration of Human Rights proclaimed by the General Assembly of the United Nations on 10th December 1948; Considering that this Declaration aims at securing the universal and effective recognition and observance of the Rights therein declared:…"
[21] The authors of the Convention began their deliberation on the basis of a 'short list' of the rights and freedoms contained in the Declaration. A. H. Robertson, 'Collected edition of the 'travaux préparatoires' of the European Convention on Human Rights = Recueil des travaux préparatoires de la Convention Européenne des Droits de l'Homme. Vol. 1 Preparatory Commission of the Council of Europe Committee of Ministers, Consultative Assembly, 11 May-8 September 1949', The Hague, Nijhoff, 1975.

rights.[22] While first generation or civil and political rights require states not to interfere with certain rights and freedoms of their citizens in an arbitrary way, socio-economic rights such as the right to education and to a standard of living, require states not to abstain from action, but to actively pursue and impose such freedoms by adopting legal measures or by taking active steps. Consequently, the original rationale for the Convention as a whole was laying down negative obligations for national states and granting negative freedom to citizens.

Of all articles contained in the Convention, these rationales are most prominent in the right to privacy under Article 8 ECHR specifying: 'Everyone has the right to respect for his private and family life, his home and his correspondence.' Already under the Declaration, it was this Article that was originally plainly titled 'Freedom from wrongful interference'.[23] Similarly, under the Convention, the right to privacy is only concerned with negative liberty, contrasting with other qualified rights in which positive freedoms are implicit, such as a person's freedom to manifest his religion or beliefs (Article 9), the freedom of expression (Article 10) and the freedom of association with others (Article 11). Moreover, Article 8 ECHR does not contain any implicit positive obligation, such as for example under Article 2, the obligation to protect the right to life, under Article 5, to inform an arrested person of the reason for arrest and to bring him or her promptly before a judge, under Article 6, the obligation to ensure an impartial and effective judicial system, and under Article 3 of the First Protocol, the obligation to hold free elections.[24]

In this line, the Court still holds that the 'essential object of Article 8 is to protect the individual against arbitrary action by the public authorities'.[25] However, the Court has gradually diverged from the original approach of the Convention authors by accepting both positive obligations for national states and granting a right to positive freedom to individuals under the right to privacy. The element of positive freedom was adopted quite early in a case from 1976: 'For numerous Anglo-Saxon and French authors the right to respect for "private life" is the right to privacy, the right to live, as far as one wishes, protected from publicity. [H]owever, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality.'[26] Likewise, from very early on, the Court has broken with the strictly limited focus of the authors of the Convention on negative obligations and has accepted that states may, under certain circumstances, be under a positive obligation to ensure respect for the Convention.[27]

[22] K. Vasak, 'Human Rights: A Thirty-Year Struggle: the Sustained Efforts to give Force of law to the Universal Declaration of Human Rights', UNESCO Courier 30:11, Paris, United Nations Educational, Scientific, and Cultural Organization, 1977.
[23] UN documents: E/HR/3.
[24] H. Tomlinson, 'Positive obligations under the European Convention on Human Rights', <http://bit.ly/17U9TDa>, p. 2.
[25] See among others: ECtHR, *Arvelo Apont v. The Netherlands*, appl.no. 28770/05, 3 November 2011, § 53.
[26] ECmHR, *X. v. Iceland*, appl.no. 6825/74, 18 May 1976.
[27] A. R. Mowbray, 'The development of positive obligations under the European Convention on Human Rights by the European Court of Human Rights', Oxford, Portland, 2004. ECtHR, Case *"Relating to certain aspects of the Laws on the Use of Languages in Education in Belgium" v. Belgium*, appl.nos. 1474/62, 1677/62, 1691/62, 1769/63, 1994/63 and 2126/64, 23 July 1968. ECtHR, *Marckx v. Belgium*, appl.no. 6833/74, 13 June 1979. ECtHR, Marzari v. Italy, appl.no. 36448/97, 4 May 1999. ECtHR, *Monory v. Hungary*, appl.no. 71099/01, 05 April 2005.

Following this line, the right to privacy is increasingly interpreted by the Court as a right that guarantees the development and expression of one's identity and personality,[28] among others by stressing 'the fundamental importance of [the protection of private life] in order to ensure the development of every human being's personality.'[29] Consequently, states are under an obligation, inter alia, to allow individuals to receive the information necessary to know and to understand their childhood and early development as this is held to be of importance because of 'its formative implications for one's personality'.[30] Moreover, the right 'to develop and fulfill one's personality necessarily comprises the right to identity and, therefore, to a name'.[31] With regard to the development and fulfilment of one's identity in the external sphere, among others, the Court has not only protected (the creation of) the family sphere,[32] it has also accepted that Article 8 ECHR 'protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world'.[33]

Subsequently, the right to privacy has been extended to the professional sphere, so that wire-tapping professional conversations, the seizures of business documents and the sanctity of the 'home' of a person's professional working place are provided protection under Article 8 ECHR.[34] This is so, according to the Court, because private life 'encompasses the right for an individual to form and develop relationships with other human beings, including relationships of a professional or business nature'[35] and because Article 8 ECHR does not exclude, in principle, 'activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world'.[36] These are but a few of the examples from which it may appear that the right to develop one's identity and personality both in private and in public, both in the personal and the professional realm has been accepted by the Court as one of the core rationales underlying the right to privacy.

2.2. The right of complaint

When drafting the ECHR, the authors of the Convention chose to link the right to petition only to a limited extent to the individual and the protection of his interests.[37] Under the ECHR, there are two complaint procedures, one for inter-state complaints and another for

[28] ECtHR, *Frette v. France*, appl.no. 36515/97, 26 February 2002.
[29] ECtHR, *Varapnickaite-Mazyliene v. Lithuania*, appl.no. 20376/05, 17 January 2012, § 43. See further: ECtHR, Biriuk v. Lithuania, appl.no. 23373/03, 25 November 2008. ECtHR, *Niene v. Lithuania*, appl.no. 36919/02, 25 November 2008.
[30] ECtHR, *Phinikaridou v. Cyprus*, appl.no. 23890/02, 20 December 2007, § 45. ECtHR, *Mikulic v. Croatia*, appl.no. 53176/99, 07 February 2002. ECtHR, *Gaskin v. the United Kingdom*, appl.no. 10454/83, 07 July 1989.
[31] ECmHR, *K.B. v. the Netherlands*, appl.no. 18806/91, 01 September 1993.
[32] See for a more general overview: U. Kilkelly, 'The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights', Human rights handbooks, 2003. <http://echr.coe.int/NR/rdonlyres/77A6BD48-CD95-4CFF-BAB4-ECB974C5BD15/0/DG2ENHRHAND012003.pdf>.
[33] ECtHR, *Pretty v. the United Kingdom*, appl.no. 2346/02, 29 April 2002, § 61.
[34] ECtHR, *Chappell v. the United Kingdom*, appl.no. 10461/83, 30 March 1989.
[35] ECtHR, *C. v. Belgium*, appl.no. 21794/93, 07 August 1996, § 25.
[36] ECtHR, *Niemitz v. Germany*, appl.no. 13710/88, 16 December 1992, § 29.
[37] The right of complaint is discussed in more detail in: B. van der Sloot, 'Privacy in the post NSA era: time for a fundamental revision?', JIPITEC, 2014-1.

individual complaints. In an inter-state procedure, it is not the personal interest of the applicant that is assessed, as the applicant state is not itself harmed in any way, nor that of anyone else, but the general quality of the actions and laws of the government accused of a violation of the Convention as such. In such cases, the applicant state brings an action against another state out of the general interest of the country's population, often related to abuse of power; although the citizens of that country may obviously be affected by the policies and/or laws, their individual injury is not central to the Court's assessment.

Moreover, the individual right of complaint may be invoked not only by natural persons, but also by legal persons (excluding governmental organizations) and groups. Typical of the latter two categories is that again, no personal harm needs to be demonstrated. A legal person may be hindered in its (business) activities, but cannot suffer personal injury or complain about a violation of its autonomy or dignity, among others. Again, in such complaints, it is usually the unlawful conduct of or the abuse of power by the government as such that is at the center of the Court's assessment. In addition, the legal capacity of groups to submit a case to the Court must be understood against the backdrop of the Second World War, in which groups were systematically discriminated against and stigmatized.[38] The authors of the Convention opened up the right to petition to a person or a group who wants to stand up for the interests of a particular group, without necessarily having suffered individually and specifically from the targeted practice, affecting the group as a whole.[39]

Finally, given the serious fear for an excessive flow of complaints by individuals,[40] the authors of the Convention decided to introduce a two-step system, in which the admissibility of applications is first reviewed by the European Commission of Human Rights (a task which has been reassigned to a separate chamber of the Court since 1998), and is only afterwards assessed by the Court on the substance of the matter. Characteristically, individuals were initially only allowed to bring complaints before the Commission but not before the Court, even if their case was declared admissible by the Commission. Only the Commission itself or a Member State could decide to send the case for substantive assessment to the Court, if they felt this was in the public interest.

The practice of the Court has however increasingly focused on complaints of individuals who can demonstrate their personal interest in a case. First, individuals have gradually been allowed to bring complaints directly before the Court.[41] As a general principle, only individuals who can demonstrate a personal interest in a procedure can successfully bring forth a claim. It follows that *in abstracto* claims that target a law or legal provision as such, without it being applied to a claimant specifically or having any other practical effect, are systematically rejected.[42] This doctrine also, in principle, excludes hypothetical complaints and *a priori* claims, regarding damage which has not yet materialized.[43] Only if the degree of probability that damage will occur is reasonable and the consequences of the act complained of are not too remote, will an exception be applied.[44] Finally, claims in the form of an *actio popularis*, in which a group or organization submits a

[38] Robertson, vol. 1, p. 160-162
[39] Robertson, vol. 2, p. 270.
[40] Robertson, vol. 2, p. 188-192.
[41] An intermediate step: <http://conventions.coe.int/Treaty/en/Treaties/Html/140.htm>.
[42] See for example: ECtHR, Popov and others, *Vakarelova, Markov* and *Bankov v. Bulgaria*, appl.nos. 48047/99, 06 November 2003.
[43] See for example: ECmHR, *Simpon v. the United Kingdom*, appl.no. 14688/89, 04 December 1989.
[44] ECmHR, *Tauira and 18 others v. France*, appl.no. 28204/95, 04 December 1995.

complaint on behalf of society, have been systematically rejected under the Convention,[45] as the claimants must have suffered from personal harm to be able to put forward a case.

In addition, the other modes of complaint have been of (almost) no value. Since the entry into force of the Convention, only about 20 inter-state complaints have been filed,[46] the possibility of a group-complaint has been limited by the Court to the opportunity of different individuals, all of whom have directly and individually suffered from a certain practice, to join their cases, and the Court has ruled that in principle, legal persons cannot rely on Article 8 ECHR. For example, when a church complained about a violation of its privacy by the police in relation to criminal proceedings, the Commission found that '[t]he extent to which a non-governmental organization can invoke such a right must be determined in the light of the specific nature of this right. It is true that under Article 9 of the Convention a church is capable of possessing and exercising the right to freedom of religion in its own capacity as a representative of its members and the entire functioning of churches depends on respect for this right. However, unlike Article 9, Article 8 of the Convention has more an individual than a collective character [].'[47]

It follows that in principle, legal persons are allowed to claim fundamental rights but not the right to privacy, as this is thought to protect the personal interests of a natural person only. This principle has been retained for a very long time. However, in its more recent jurisprudence, the Court is willing to accept some exceptions. Four situations should be distinguished. First, the situation in which a legal person represents natural persons in an official complaint. This situation is seems unproblematic to the Court; legal persons are usually held to have standing (*locus standi)* to submit such complaints. They must, however, be able to show that they have received a specific mandate from natural persons to represent them in legal proceedings. An association may represent its members but only in a way a lawyer would represent its clients, being specifically instructed by each of them to represent their interests.[48]

Second, in principle, neither natural nor legal persons may bring forth a claim on behalf of the general interest, i.e. a class action or *actio popularis.* Still, in more recent case law, the Court is increasingly willing to allow for exceptions. This is particularly so in cases which involve mass surveillance practices by governmental agencies and secret services. Here the victim requirement is relaxed. For example, in a case involving a presumed surveillance practice about which no insight was given by the secret services, the Court held that it is unacceptable that 'the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation.'[49] Thus, although the applicant could not demonstrate with certainty that he was directly affected by surveillance practices, he was allowed to bring forth a claim. Similarly, the Court has in some cases also been prepared to adopt a broader interpretation with regard to complaints about legislation authorizing surveillance practices which is drafted in very broad and general terms, by determining that '[t]he mere existence of the legislation

[45] ECmHR, *X. v. the United Kingdom*, appl.no. 8416/78, 13 May 1980.
[46]
<http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx#{"article":["33"],"documentcollectionid2":["JUDGMENTS","DECISIONS"]}>.
[47] ECmHR, Church of Scientology of *Paris v. France*, appl.no. 19509/92, 09 January 1995.
[48] ECmHR, Asociacion de Aviadores de la Republica, *Mata et al. v. Spain*, appl.no. 10733/84, 11 March 1985. ECtHR, *Asselbourg and 78 others and Greenpeace association-Luxembourg v. Luxembourg*, appl.no. 29121/95, 29 June 1999.
[49] ECtHR, *Klass and others v. Germany*, appl.no. 5029/71, 06 September 1978, § 36.

entails, for all those who might fall within its reach, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunications services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for correspondence.'[50] In such cases, the Court also allows both natural and legal persons to rely on Article 8 ECHR and claim that they have suffered from a privacy violation.[51]

Third, the interests of a company may have a direct impact on the interests of a natural person. The transformation of the right to privacy to a personality right has resulted in a widened scope of Article 8 ECHR. The protection of 'private and family life' includes the possibility of creating and maintaining social contacts in general and to develop one's identity to the fullest, inter alia, in the professional sphere. Similarly, the Court has ruled that 'home' must be understood as also applying to business premises, especially in the case of one man businesses which operate from the home of the owner. Likewise, the secrecy of communication, as guaranteed by Article 8 ECHR, is held by the Court to extent to professional communications.[52] The Court has held, among other cases, in its *Chappell* and *Niemitz* judgments, that there is no reason of principle why the notion of private life should be taken to exclude activities of a professional or business nature. 'This view is supported by the fact that [] it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not. Thus, especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time.'[53] Thus, the professional life of an applicant and the interests of a legal person (for example his one-man business) may also affect a person's private life and consequently form a part of his personal interest.

Fourth and finally, the Court has gradually accepted that this line should be extended to legal persons as such, who may invoke a right to privacy to protect their own interests. In a case from 2002, *Colas v. France*, a business complained about the searches and seizures of the government on their business premises. 'In *Chappell v. the United Kingdom*, the Court considered that a search conducted at a private individual's home which was also the registered office of a company run by him had amounted to interference with his right to respect for his home within the meaning of Article 8 of the Convention. The Court reiterates that the Convention is a living instrument which must be interpreted in the light of present-day conditions. [] Building on its dynamic interpretation of the Convention, the Court considers that the time has come to hold that in certain circumstances the rights guaranteed by Article 8 of the Convention may be construed as including the right to respect for a company's registered office, branches or other business premises.'[54] In later jurisprudence, the ECtHR has confirmed that businesses may successfully invoke a right to privacy.

2.3. The protection of legal persons' privacy concerns

[50] ECtHR, *Lordachi and others v. Moldavia*, appl.no. 25198/02, 10 February 2009, § 34. ECtHR, Liberty v. Great Britain, appl.no. 58243/00, 01 July 2008, § 57.
[51] The Court however (rather artificially) seems to retain the principle of personal harm, but suggests that with such legislation and practices, everybody is harmed and can thus invoke Article 8 ECHR.
[52] ECtHR, *Chappell v. the United Kingdom*, appl.no. 10461/83, 30 March 1989. ECtHR, *C. v. Belgium*, appl.no. 21794/93, 07 August 1996, § 25.
[53] Niemitz, § 25.
[54] ECtHR, *Stes Colas Est and others v. France*, appl.no. 37971/97, 16 April 2002, § 40-41.

Legal persons are thus allowed to claim a right to privacy (Article 8 ECHR), not only to protect the interests of others, but also to protect their own (business) interests. However, it must be stressed that they do not enjoy protection similar to natural persons. Marius Emberland, who has made a careful analysis of the *Colas* judgment, suggests that the ECtHR provides substantially less protection for legal persons than for natural persons: 'the court considered that juristic persons should not be able to assert a right to protection for commercial premises with the same intensity as individuals could for premises utilized for the exercise of a liberal profession (as was the case in *Niemietz).* In other words, public authorities, under the necessity test, should be allowed to interfere with the "home" rights of a company to a greater degree than they could with the same rights of individuals.'[55]

First, it should be stressed that the cases in which legal persons are allowed to invoke Article 8 ECHR are still very scarce. It appears that there are a dozen or so in which the Court has allowed legal persons to bring forth a claim relying on article 8 ECHR. These cases, without exception, regard traditional privacy concerns, namely the entry of business premises by governmental officials, the confiscation of professional documents and the wire-tapping of company correspondence, data collection and surveillance, etc.[56] This is similar to the 'classic' privacy concerns for which Article 8 ECHR was installed, namely to protect the citizen from arbitrary governmental interference through wire-tapping, the entry of homes or the confiscation of personal belongings. Such concerns are now transposed to legal persons.

These cases not only involveclassic privacy issues, they also only entail negative obligations. In reference to natural persons, the Court has often said that states should take active measures to ensure a person's privacy and respect for one's family life, home and communications, by adopting specific legislation or taking concrete actions.[57] Such positive obligations have so far not been accepted in cases in which legal persons relied on Article 8 ECHR. Moreover, with regard to natural persons, the Court has often held that the state has a positive obligation to ensure respect for a person's privacy in horizontal relations, that is not between citizen and state (vertical relation), but between citizens and/or companies.[58] For example, the state may have an obligation to return a child which is abducted by a parent, to guarantee the respect for a person's family life. The respect for the privacy of legal persons has however so far not been applied to horizontal relationships.

---

[55] M. Emberland, 'Protection Against Unwarranted Searches and Seizures of Corporate Premises under Article 8 of the European Convention on Human Rights: The Colas Est SA v. France Approach, 25 Michigan Journal of International Law, 77 2003 82, p. 102. The term 'two-tiered', also used in this publication, is coined by Emberland. See further:
<http://www.mcgeorge.edu/Documents/Conferences/GlobeJune2012_Corporationsandthe.pdf>.

[56] See besides Colas Est, inter alia: ECtHR, *Saint-Paul Luxembourg S.A. v. Luxembourg*, appl.no. 26419/10, 18 April 2013. ECtHR, *Bernh Larsen Holding AS and others v. Norway*, appl.no. 24117/08, 14 March 2013. ECtHR, *Wiese rand Bicos Beteiligungen GMBH v. Austria*, appl.no. 74336/01, 16 October 2007. ECtHR, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, appl.no. 62540/00, 28 June 2007. ECtHR, André and another v. France, appl.no. 18603/03, 24 July 2008. ECtHR, Liberty and other v. the United Kingdom, appl.no. 58243/00, 01 July 2008. ECtHR, *Ernst and others v. Belgium*, appl.no. 33400/96, 15 July 2003. See however also, inter alia: ECtHR, *Vallianatos and others v. Greece*, appl.nos. 29381/09 and 32684/09, 07 November 2013. ECtHR, *Winterstein and others v. France*, appl.no. 27013/07, 17 October 2013. ECtHR, *Avilkina and others v. Russia*, appl.no. 1585/09, 06 June 2013.

[57] A. R. Mowbray, 'The development of positive obligations under the European Convention on Human Rights by the European Court of Human Rights', Oxford, Portland, 2004.

[58] L. F. M. Verhey, 'Horizontal effect of fundamental rights, in particular the right to privacy', Tjeenk Willink, Zwolle, 1992. [L. F. M. Verhey, 'Horizontale werking van grondrechten, in het bijzonder van het recht op privacy', Tjeenk Willink, Zwolle, 1992.]

Perhaps most importantly, given the transformation of Article 8 ECHR from a negative right to a personality right, the individual is granted a (very) wide range of rights and freedoms. It goes too far to describe which implications this development has had for the scope of the right to privacy, but in general it seems that Article 8 ECHR provides the individual with protection of virtually everything that directly or indirectly relates to the individual, his interests and his development. For example, rights are granted to found a family,[59] to protect a person's honor and reputation,[60] to protect property and work,[61] to beget a residence permit,[62] to live in a clean and healthy living environment[63] and to protect minorities and their minority life style and identity.[64] These are but a few of the rights and freedoms granted to natural persons under Article 8 ECHR. These 'new' rights have however (so far) only been applied to individuals and never to legal persons. Legal persons cannot rely on Article 8 ECHR to protect their honor and reputation, invoke a right to found a family, to a clean and healthy living environment or the protection of their minority culture, among other rights. Thus there is a clear difference between the marginal level of protection granted to legal persons and the (very) wide range of rights and freedoms of natural persons under the right to privacy, as interpreted by the European Court for Human Rights.

2.4. Conclusion to section 2

Three points have been made in this section. First, the material scope of the right to privacy has extended quite considerably. Originally, privacy rules were focused on laying down rules of good governance and safeguards against the abuse of power. Privacy, originally, primarily entailed an obligation for states not to abuse their power, that is, not to mingle with the private sphere of citizens, enter their home or interfere with their personal communication, when this is not necessary, proportional or effective or without legal basis. However, it has undergone a significant change. More emphasis has been placed on the protection of natural persons and their private interests, among others things, by giving them a number of subjective rights. Under the ECHR, the right to privacy has transferred from a negative right to a full fletched personality right, granting the individual protection to almost every aspect of his life.

Second, although the Convention allows for a different interpretation, the Court has only granted protection to natural persons under the scope of the right to privacy. In more recent years, however, legal persons are also able to invoke Article 8 ECHR to protect their own interests, after a judgment from 2002 (Colas). Strange as it may sound, this seems partly a consequence of the increased focus on the natural person, his private interests and the full development of his personality. In the early jurisprudence of the former Commission and the Court, it was held that a second home, a building site, a professional working place, a temporary shelter or other unconventional houses did not fall under the scope of 'home'. For

[59] See among others: ECtHR, *Evans v. the United Kingdom*, appl.no. 6339/05, 10 April 2007. ECtHR, *Dickson v. the United Kingdom*, appl.no. 44362/04, 04 December 2007.
[60] See among others: ECtHR, *Pfeifer v. Austria*, appl.no. 12556/03, 15 November 2007. ECtHR, *Rothe v. Austria*, appl.no. 6490/07, 04 December 2012. ECtHR, *A. v. Norway*, appl.no. 28070/06, 09 April 2009.
[61] See among others: ECtHR, *Oleksandr Volkov v. Ukraine*, appl.no. 21722/11, 09 January 2013.
[62] See among others: ECtHR, *Sen v. the Netherlands*, appl.no. 31465/96, 21 December 2001.
[63] See among others: ECtHR, *López Ostra v. Spain*, appl.no. 16798/90, 09 December 1994. ECtHR, *Fadeyeva v. Russia*, appl.no. 55723/00, 09 June 2005. ECtHR, *Ledyayeva, Dobrokhotova, Zolotareva and Romashina v. Russia*, appl.nos. 53157/99, 53247/99, 56850/00 and 53695/00, 26 October 2006.
[64] See among others: ECtHR, *Chapman v. the United Kingdom*, appl.no. 27238/95, 18 January 2001. ECtHR, *Aksu v. Turkey*, appl.nos. 4149/04 and 41029/04, 27 July 2010. ECtHR (Grand Chamber), *Aksu v. Turkey*, appl.nos. 4149/04 and 41029/04, 15 March 2012.

example, with regard to the search of a person's car, which functioned as his home, the Commission held: '[] la Commission estime que le domicile - "home" - dans le texte anglais de l'article 8 (art. 8)- est une notion précise qui ne pourrait être étendue arbitrairement et que, par conséquent, la fouille de la voiture en stationnement dans les circonstances de la présente affaire, ne saurait être assimilée à une fouille dimiciliaire qui entre dans le domaine d'application de l'article 8 (art. 8).'[65] However, the Convention is drafted in two official languages, English and French, and the French version of the European Convention does not refer to 'maison', 'chez' or 'residence' but rather to the concept 'domicile'. Domicile has a broader scope than the concept of 'home' and might, for example, be used to refer to professional dwellings.

In its recent jurisprudence, the Court has increasingly referred to this French concept and has held as a principle that the concept of 'home' is not limited to those buildings which are lawfully occupied or which have been lawfully established.[66] Furthermore, it has accepted caravans and other mobile homes and temporary shelters under the concept of 'home', which has had important consequences for Gypsies and other nomadic groups,[67] who generally do not possess a fixed shelter or home.[68] Building on this line of interpretation, the Court has accepted that individuals who work from home also fall under the scope of Article 8 ECHR, that the interests of one-man firms may be part and parcel of the interest of the natural person and that consequently, entering a business premises (by the police) may affect the right to privacy of a natural person. Building on this interpretation the Court has accepted not only that a business of a natural person may fall under the protection of 'home' under Article 8 ECHR, but also that businesses as such may seek protection under the right to privacy as guaranteed under the ECHR. Still, there exist some limitations on this principle. Among others, the Commission and the Court have been reluctant to include public places, such as inns, bars and restaurant, under the concept of either private life or home[69] and not all business premises can fall, ratione materiae, under the extended concept of 'home', such as piggeries and farms housing several hundred pigs.[70]

Third and finally, in those cases in which they are able to invoke 8 ECHR, legal persons are only allowed partial protection. Under Article 8 ECHR, legal persons may only bring forth a complaint regarding the wire-tapping of their communication channels, the confiscation of business documents and the illegal entry of their premises by governmental officials. The scope of the protection is limited to negative obligations by the state in vertical relations. Legal persons are not allowed to invoke any of the 'new' rights, as acknowledged by the Court. Consequently, their claims are only accepted if they coincide with a societal interest, namely the prevention of the abuse of power, not when they regard a purely 'personal' interest. Section 4 of this article will analyze whether this is a positive development and argue that a two-tiered system in the protection of privacy could be

[65] ECmHR, *X. v. Belgium*, appl.no. 5488/72, 30 May 1974.
[66] ECtHR, *McKay-Kopecka v. Poland*, appl.no. 45320/99, 19 September 2006. ECtHR, *McGonnell v. UK*, appl.no. 28488/95, 08 February 2000.
[67] ECmHR, *Lay v. UK*, appl.no. 13341/87, 14 July 1988.
[68] ECmHR, *Smith v. UK*, appl.no. 14455/88, 04 September 1991. ECmHR, *Smith v. UK*, appl.no. 18401/91, 06 May 1993.
[69] See further: ECmHR, *Schuschou v. Austria*, appl.no. 22446/93, 16 January 1996. ECmHR, *Garcia Sousa v. Spain*, appl.no. 33371/96, 21 May 1997. ECtHR, *Steel and Morris v. the United Kingdom*, appl.no. 68416/01, 22 October 2002. ECmHR (report), *Pentidis, Katharios and Stagopoulos v. Greece*, appl.no. 23238/94. ECtHR, R.L. and *M.-J.D. v. France*, appl.no. 44568/98, 18 September 2003.
[70] ECtHR, *Leveau and Fillon v. France*, appl.nos. 63512/00 and 63513/00, 06 September 2005.

envisaged: one for privacy as a doctrine that (primarily) protects a societal value, one for privacy as a doctrine that (primarily) protects an individual value.

3. The right to data protection

3.1. The scope of the right to data protection

With the Charter of Fundamental Rights of the European Union from 2000,[71] entering into force in 2009,[72] in which the right to data protection is contained in a provision (article 8) separated from the right to privacy (article 7), and the plans to adopt a European Union wide General Data Protection Regulation, the still young right to data protection seems to have reached the point of maturity.[73] Its origins lie partially in the data protection rules of northern European countries arising in several countries in the seventies of the last century[74] and partially in the U.S. and the realization of the so called Fair Information Practices (FIPs), which were developed because the right to privacy was thought unfit for the 'modern' challenges posed by large automated data processing.[75] The increased use of large data bases by (primarily) governmental organisations raised a number of problems for the traditional conception of the right to privacy, which by then primarily aimed at protecting the private interests of the citizen, among others, by giving him a right to control private and sensitive data.[76]

First, data processing often does not involve private or sensitive data, but public and non-sensitive data such as car ownership, postal codes, number of children, etc.[77] 'Dictionary definitions of privacy uniformly speak in terms of seclusion, secrecy, and withdrawal from public view. They all denote a quality that is not inherent in most record-keeping systems', one of the U.S. governmental reports from 1973 established.[78] Secondly, and related to that, the traditional privacy definitions emphasized the right 'of the data subject as having a unilateral role in deciding the nature and extent of his self-disclosure. None accommodates the observation that records of personal data usually reflect and mediate relationships in which both individuals and institutions have an interest, and are usually made for purposes that are shared by institutions and individuals.'[79] Both concerns were also at the centre of the

[71] <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.
[72] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, 2007/C 306/01.
[73] The points on the scope of the right to data protection are discussed in more detail in: B. van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the General Data Protection Regulation', International Data Privacy Law, forthcoming.
[74] U. Dammann, O. Mallmann & S. Simitis (eds.), 'Data protection legislation: an international documentation: Engl.-German : eine internationale Dokumentation = Die Gesetzgebung zum Datenschutz', Frankfurt am Main, Metzner, 1977.
[75] See among others: Personal privacy in an Information Society. The Report of the Privacy Protection Study Commission, July 1977. Privacy online: A report to congress. Federal Trade Commission, June 1998.
[76] See also: The Privacy Act of 1974 5 U.S.C. § 552a. See further: H. Burkert, 'Freedom of information and data protection', Bonn, Gesellschaft für Mathematik und Datenverarbeitung, 1983.
[77] See for the distinction between 'private' and 'personal' data: R. Wacks, 'Personal Information: Privacy and the Law', Oxford, Clarendon Press, 1989, p. 21-25. See for the 'private' and 'public' distinction among others: S. Strömholm, 'Right of Privacy and Rights of the Personality', Stockhol, P.a. Norstedt & Söners Förlag, 1967, p. 65-75.
[78] Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July, 1973.
[79] Records, Computers and the Rights of Citizens (1973).

early European legislation of different (northern-European) countries[80] and of the two data protection Resolutions adopted in 1973 and 1974 by the Council of Europe.[81]

Because data processing often does not concern private and sensitive data, the right to control by the data subject was felt neither legitimated by his private interests nor feasible. This is because Governments need such general data to develop, among others things, adequate social and economic policies. Consequently, instead of granting a right to control, the focus of the early data protection instruments was on the fairness and reasonableness of the data processing, for example by specifying that data should not be collected and processed when this was not necessary for or proportionate to the goal pursued and by laying down that the data should be correct and kept up to data, so as to guarantee that the profile of a person or a group of people was accurate.[82] Data processers were also encouraged to publish an annual public notice which contained, inter alia, the nature and purpose of the data system, the categories and number of persons on whom data are maintained, the categories of data maintained, the organization's policies and practices regarding data storage, duration of retention of data, and disposal thereof.[83]

Under the Data Protection Directive, two important changes have been made to these two fundaments of early data protection instruments. First, the transparency principle is retained, but in a quite different form. There is on the one hand the obligation to notify the national Data Protection Authority (DPA) about the processing of personal data, although Member States are at liberty to adopt quite far-reaching exemptions. On the other hand, there is a duty to notify the data subject itself about the data processing activities. Thus, article 10 specifies that the controller must provide a data subject from whom data relating to him are collected with at least information regarding the identity of the controller, the purposes of the processing for which the data are intended and the recipients of the data.[84] Consequently, the transparency principle is transformed from a duty to notify the public, to a duty to notify the data subject himself. Secondly, the obligations of fairness are broadened. The principles of fair and lawful, safe and confidential data processing, of data quality and special care for sensitive data, among others, have all been transposed to the Directive. New is that it stipulates six grounds for legitimate data processing, such as the informed consent of the data

[80] F. W. Hondius, 'Emerging data protection in Europe', Amsterdam, American Elsevier Pub. Co, 1975. Organisation for Economic Co-operation and Development, 'Policy issues in data protection and privacy: concepts and perspectives: proceedings of the OECD seminar, 24th to 26th June 1974', Paris, Organisation for Economic Co-operation and Development, 1976. H. Burkert, 'Freedom of information and data protection', Bonn, Gesellschaft für Mathematik und Datenverarbeitung, 1983.

[81] Council of Europe. Committee of Ministers, Resolution (73) 22 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the private sector. (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies). Council of Europe. Committee of Ministers, Resolution (74) 29 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the public sector. (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies).

[82] See further: A. F. Westin & M. A. Baker, 'Databanks in a Free Society: Computers, Record-keeping and priacy', New York, Quadrangle, 1972.

[83] See among others: Organisation for Economic Co-operation and Development, 'Policy issues in data protection and privacy: concepts and perspectives: proceedings of the OECD seminar, 24th to 26th June 1974', Paris, Organisation for Economic Co-operation and Development, 1976. H. Burkert, 'Freedom of information and data protection', Bonn, Gesellschaft für Mathematik und Datenverarbeitung, 1983. However, the Resolution from 1973 does not embody a similar transparency principle. Council of Europe. Committee of Ministers, Resolution (73) 22 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the private sector. Council of Europe. Committee of Ministers, Resolution (74) 29 On the Protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.

[84] Article 10 Data Protection Directive. See also: Article 11 Data Protection Directive.

subject, a legal contract or legal obligation and when the interests of the controller to process the data outweigh those of the data subject.

With the proposed General Data Protection Regulation,[85] which will replace the Directive over time, a strong emphasis on the element of consent and the control of the subject over his personal data seems at hand.[86] The definition of consent has been tightened[87] and it has been clarified that the controller shall bear the burden of proof for the data subject's consent.[88] Secondly, the controller will be under a general 'accountability duty'.[89] This duty is used as an umbrella concept under which falls a myriad of obligations, such as the keeping of very detailed and precise documentation on all processing operations, making data protection impact assessments,[90] assessing the risk concerned with certain types of data processing, on the basis of which, among others, further and stronger technical measures may need to be taken,[91] the obligation to appoint a data protection officer, etc.[92] Perhaps most importantly, the principle of transparency has been almost completely lost. The obligation of a general notification to the supervisory authority has been replaced by the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility[93] and the obligation to inform the data subject about data processing has been replaced by the obligation to provide transparent and easily accessible and understandable information with regard of the data processing.[94] Only when a data breach has occurred does the controller have an active obligation to inform the data protection authorities,[95] and only when this will have an adverse effect on the interests of the data subjects will they be directly informed.[96]

During the years, the material scope of the data protection rules has grown considerably and so has the number and the width of the subjective rights granted to the data subject. Previous to the Data Protection Directive, most data protection instruments only contained two marginal rights by the data subject. First, the right to have access to the data stored by the data processor and second the right to request correction when the data where incorrect, incomplete or out of date.[97] The Data Protection Directive expanded this list and specified three subjective rights by the data subject. One contained the right of access to personal data, i.e. begetting information about the data processing of his personal data (which

[85] For the sake of clarity and conciseness, reference will be made only to the original proposal of the Commission. At the time of writing the adoption and final result of the Regulation is still uncertain.
[86] F. Gilbert, 'EU Data Protection Overhaul: New Draft Regulation', The Computer & Internet Lawyer 2012-3, p. 3. P. De Hert & V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', [2012] 28 Computer Law & Security Review 130 at p. 137-138. G. Hornung, 'A General Data Protection Regulation for Europe? Light and Shade in the Commissions Draft of 25 January 2012', Script*ed* 2012-1, p. 74.
[87] Article 4 (8) European Commission Proposal (2012). Compare Article 2 (h) Data Protection Directive.
[88] Article 7 European Commission Proposal (2012).
[89] Article 22 European Commission Proposal (2012).
[90] Article 33 European Commission Proposal (2012). See already for risk assessments: R. Sizer & P. Newman, 'The Data Protection Act: a practical guide', Gower, Aldershot, p. 188-193.
[91] Article 30 European Commission Proposal (2012).
[92] This does not apply to small companies. Article 35 European Commission Proposal (2012).
[93] Article 28 European Commission Proposal (2012).
[94] Article 11 European Commission Proposal (2012).
[95] Article 31 European Commission Proposal (2012).
[96] Article 32 European Commission Proposal (2012).
[97] U. Dammann, O. Mallmann & S. Simitis (eds.), 'Data protection legislation: an international documentation: Engl.-German: eine internationale Dokumentation = Die Gesetzgebung zum Datenschutz', Frankfurt am Main, Metzner, 1977.

data, who processes them, why, etc.)[98] and the right to communication to him in an intelligible form the data undergoing processing.[99] Second, the data subject has a right to rectification, erasure or blocking of personal data, the processing of which does not comply with the data protection rules[100] and a right to object to the processing of his personal data.[101] Third and finally, every person has a right to object to an automatic decision making process; this right, however, only applies when a number of conditions have been met.[102]

With the proposal for a General Data Protection Regulation, a shift seems at hand. The right to access personal information has been broadened by stressing, among others, the right to be informed about the storage period.[103] A new right is introduced, which is partially based on the data subject's right to obtain the personal data being processed about him, that specifies the data subject's right to data portability, i.e. to transfer data from one electronic processing system to and into another.[104] It provides the right to obtain from the controller his personal data in a structured and commonly used electronic format, for example facilitating the transfer from Facebook to another social network.[105] The regulation goes even further and stresses not only the subject's right to rectification,[106] but also introduces a right to be forgotten,[107] which grants the data subject the right to obtain from the controller the erasure of personal data relating to him and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child.[108] Finally, the rights to object and resist automatic processing have been extended quite considerably,[109] the latter being transformed into a right to object to profiling in general, and a number of thresholds for invoking this right have been removed.[110]

In conclusion, both with regard to privacy and to data protection, there seems to be a shift from an obligation based doctrine, emphasizing rules of good governance and duties of care, to a rights based model, from a doctrine that aims at safeguarding societal interests, such as the legitimacy of the state (not abusive of its power) and the integrity of data processing systems, to a model that aims at preserving specific individual interests, and from a doctrine that is aimed at intrinsic limits on the use of power by either the state or the data controller to

[98] See also: ECJ (Grand Chamber), Heinz Huber v Bundesrepublik Deutschland, 16 December 2008, Case C-524/06.
[99] Article 12 Data Protection Directive.
[100] Article 12 Data Protection Directive.
[101] Article 14 Data Protection Directive.
[102] Article 15 Data Protection Directive.
[103] Article 15 European Commission Proposal (2012).
[104] S. Weiss, 'Privacy threat model for data portability in social network applications', International Journal of Information Management 2009-29. U. Bojars, A. Passant, J. G. Breslin & S. Decker, 'Social Network and Data Portability using Semantic Web Technologies', <http://ceur-ws.org/Vol-333/saw1.pdf>.
[105] Compare to number portability: Article 30 Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)
[106] Article 16 European Commission Proposal (2012).
[107] See also the prior version: <http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf>.
[108] I. Szekely, 'The right to forget, the right to be forgotten: Personal Reflections on the fate of personal data in the information society'. In: S. Gutwirth, R. Leenes, P. De Hert & Y. Poullet, European Data Protection: In Good Health?, Dordrecht: Springer 2012. S. C. Bennett, 'The "Right to be Forgotten": Reconciling EU and US Perspectives', Berkeley Journal of International Law 2012-30.
[109] Article 19 European Commission Proposal (2012).
[110] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies).

a model in which the individual interest is increasingly weighed and balanced against the societal interest, such as security and economic welfare. This has had a clear impact on the scope of both the right to privacy and that of data protection.

3.2. The right of complaint

The Council of Europe adopted two Resolutions for data processing in 1973 and 1974, one for the public and one for the private sector, which defined 'personal information' simply as information relating to individuals (physical persons). Here, the individual and subjective element in the definition of personal data is still prominent. Already in 1981, however, in the subsequent Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Council of Europe, 'personal data' was defined as any information relating to an identified or identifiable individual.[111] The explanatory report stressed that an 'identifiable person', an element which was new to this definition, meant a person who can be easily identified; it did not cover identification of persons by means of very sophisticated methods.[112] Still, data which were not yet linked to an individual, but could be with relative ease, fell under the scope of the definition.[113]

In the Data Protection Directive of the European Union, at the suggestion of the Parliament,[114] the definition of personal data was broadened by specifying that 'an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'[115] It not only introduces a very wide, and non-exhaustive, list of possible identifying factors, the possibility of 'indirect' identifiable data was also inserted.[116] The Article 29 Data Protection Working Party

[111] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, article 2 sub a.

[112] <http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm>.

[113] A reviewer has suggested that this seems to imply that any data capable of being linked to a person at some future time would be personal even before the link was established and therefore subject to regulation even though no individual could assert rights of subject access or any other rights in respect of it. "Such a proposition has consequences: so it might be said that that the colour of the walls of the room in which I am currently sitting as I write to you – yellow in this case – is personal data relating to me and that would be true even if I could not be named, but just singled-out as the person sitting in the room with yellow painted walls. That is probably not contentious, but if the sentence in question means what I suspect then the fact that the walls of the room are coloured yellow would be personal data simply because I or someone else might at some future time come into the room." This is a difficult and interesting question. Probably, it depends on the circumstances of the case, as always. The common approach is to take the data subject as starting point and then ask which data are linked to him or could be. For example, we know that person X has a certain disease but we have not identified x. If this could be done with relative easy, this datum may be regarded as personal data. Similarly, suppose we know that a group of 100 people has a certain disease, but we do not know yet who belongs to this group. If this could be established with the use of relatively little effort, this might count as personal data. Perhaps even the situation in which a person is identified and has an established 86% probability of getting a certain disease in the future, this might be regarded as (sensitive) personal data, even though this hypothetical situation has not yet materialized. What the reviewer now proposes is not to take the data subject as starting point, but the datum itself. The yellowness of the walls or the existence of a certain disease – they can be and will be linked to an individual at some point in time and may say something about him and thus could be regarded as personal data. The easy way out would be to say that this datum is only regarded as personal data because I or any other person is in the room or has a, for example, 86% probability of walking in that yellow room. I'm not sure whether we could take the yellowness of the wall as starting point and link it to the fact that it has a 100% probability of being linked to a person or a 15% chance of being linked to person X. This deserves further research.

[114] No C94/176, Official Journal of the European Communities, 13 April 1992.

[115] Article 2 sub a Data Protection Directive.

[116] This was even broadened further: ECJ (Third Chamber), Worten – Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT), 30 May 2013, Case C-342/12.

(Working Party), the advisory body installed by the Data Protection Directive, has clarified that this suggests that even 'ancillary information, such as "the man wearing a black suit" may identify someone out of the passers-by standing at a traffic light. So, the question of whether the individual to whom the information relates is identified or not depends on the circumstances of the case.'[117] Finally, this trend of a widening scope of the definition may also be witnessed[118] in the proposal for a General Data Protection Regulation, in which personal data is defined in a slightly broader manner. The reason for this, as is acknowledged by the Working Party and is increasingly emphasized by scholars, is that potentially all data could be(come) personal data. Data which at one moment in time may contain no information about a specific person whatsoever may in the future be used, through the use of advanced techniques and the interconnection of databases, to identify or individualize a person.[119] Thus potentially all data could become personal data.

As long as the definition of personal data was linked explicitly to the physical person and required that data should directly identify him, legal persons could in principle not invoke a right to data protection. However, in more recent years, given the widening scope of the definition of 'personal data', increasingly exceptions are made to this principle.[120] Again it is important to distinguish between four situations, as already referred to when discussing the right to privacy. First, the situation in which a legal person represents a natural person in an official complaint. Second, the possibility of bringing forth a complaint on behalf of the general public or the society – the class action. Third, the situation in which the interests of a legal person are part and parcel of the interests of a natural person. Fourth, the situation in which a legal person can bring forth a complaint to protect its own interests. With regard to the first situation, as with the right to privacy, it seems to be regarded as rather unproblematic to allow legal persons to represent clients, being natural persons, in a claim regarding data protection.

Secondly, with regard to the capacity of legal persons to engage in a class action, relying on a general, societal interest, it seems that the Member States to the European Union have implemented the Directive in different ways. Accordingly, some countries prohibit such class actions and others allow it. As an example, reference can be made to a recent judgment in the Netherlands regarding a claim by a societal organization 'Privacy First' who claimed that the storage of biometric data by the government, in connection to issuing passports, was neither necessary nor proportionate. The District Court argued that Privacy First could not claim to be a victim, as it has no biometric data and because it merely represented the combined interests of all natural persons directly affected by the practices, who could have engaged in legal proceedings themselves. The claim by Privacy First was consequently

[117] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data', 01248/07/EN, WP 136, 20 June 2007, Brussels, p 13.
[118] Article 4 (1) European Commission Proposal (2012).
[119] D. Skillicorn, 'Knowledge Discovery for Counterterrorism and Law Enforcement', Boca Raton, Taylor & Francis Group, LLC 2009. D.T. Larose, 'Data mining methods and models', New Yersey, John Wiley & Sons, 2006. M. Hildebrandt & S. Gutwirth (reds.), 'Profiling the European Citizen Cross-Disciplinary Perspectives', New York, Springer 2008. C. Westphal, 'Data mining for Intelligence, Fraud & Criminal Detection', Boca Raton, Taylor & Francis Group, 2009. K. Guzik, 'Discrimination by Design: Data Mining in the United States's "War on Terrorism", Surveillance & Society 2009-7. P. Kuhn, 'Sex discrimination in labor markets: The role of statistical evidence', The American Economic Review 1987-77. M. LaCour-Little, 'Discrimination in mortgage lending: A critical review of the literature', Journal of Real Estate Literature, 1999-7. G. D. Squires, 'Racial profiling, insurance style: Insurance redlining and the uneven development of metropolitan areas', Journal of Urban Affairs, 2003-25.
[120] The best analysis on this topic can be found in: L. A. Bygrave, 'Data Protection Law: Approaching Its Rationale, Logic and Limits', Kluwer Law International, The Hague, 2002.

declared inadmissible.[121] The Court of Appeal, however, argued that it did have a legitimate interest because its founding charters specified that the organization served to protect and preserve the societal interest in relation to privacy.[122] The claim was thus declared admissible.

In the new General Data Protection Regulation, as proposed by the Commission, both the possibility of representing a natural person and engaging in a class action by legal persons are explicitly acknowledged. It holds that every data subject shall have the right to lodge a complaint with a supervisory authority if they consider that the processing of personal data relating to them does not comply with this Regulation. Moreover, it specifies that 'anybody, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.'[123] It continues by pointing out that such a body, organization or association, independently of a data subject's complaint, shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.

A natural person has two additional rights. First, the Regulation specifies that each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint.[124] Second, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.[125] However, the Regulation also specifies that anybody, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to exercise these two rights on behalf of one or more data subjects. Likewise, each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.[126]

Thirdly, as with privacy, especially for one-man businesses or relatively small firms, the processing of data about the company may indirectly identify a natural person or be used to create a profile of him. For example, the Working Party 29, has stressed that information about legal persons may also be considered as 'relating to' natural persons on their own merits. 'This may be the case where the name of the legal person derives from that of a natural person. Another case may be that of corporate e-mail, which is normally used by a certain employee, or that of information about a small business (legally speaking an "object" rather than a legal person), which may describe the behaviour of its owner. In all these cases,

[121] <http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2011:BP2860>.
[122] <http://bureaubrandeis.com/wp-content/uploads/2014/02/20140218-arrest-Hof-Den-Haag-geanonimiseerd.pdf>.
[123] Article 73 (2) European Commission Proposal (2012).
[124] Article 74 (2) European Commission Proposal (2012).
[125] Article 75 European Commission Proposal (2012).
[126] Article 76 European Commission Proposal (2012).

where the criteria of "content", "purpose" or "result" allow the information on the legal person or on the business to be considered as "relating" to a natural person, it should be considered as personal data, and the data protection rules should apply.'[127]

Reference could also be made to the e-Privacy Directive of 2002, the lex specialis of the Data Protection Directive (95/46/EC) for the electronic environment. Article 1 specifies: 'The provisions of this Directive particularize and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are *legal persons*.'[128] However, a recital to the e-Privacy Directive clarifies: 'Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.'[129] Consequently, Member States are allowed to adopt their own interpretation of those rules and subsequently have done so in a variety of ways.[130]

The Citizens' Rights Directive of 2009, amending the e-Privacy Directive, has made particularly clear that the rules regarding unsolicited communication and spam also apply to legal persons, pointing out that member States must 'also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.'[131] Moreover, it has been stressed that 'any natural or legal person adversely affected by infringements of national provisions adopted pursuant to this Article and therefore having a legitimate interest in the cessation or prohibition of such infringements, including an electronic communications service provider protecting its legitimate business interests, may bring legal proceedings in respect of such infringements. Member States may also lay down specific rules on penalties applicable to providers of electronic communications services which by their negligence contribute to infringements of national provisions adopted pursuant to this Article.'[132] Especially the last point brings with it that not only do businesses have a derived interests to protect their users against spam; as this may also directly have an impact the attractiveness of their services, they also have an own and independent legitimate interest in invoking such rules.

[127] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data', 01248/07/EN, WP 136, 20 June 2007, Brussels, p. 23-24.
[128] Emphasis added. Article 1 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[129] Recital 12 e-Privacy Directive.
[130] See on the e-Privacy Directive also: Y. Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?', in: S. Gutwirth, Y. Poullet & P. De Hert, 'Data Protection in a Profiled World, Springer, Dordrecht, 2010.
[131] Article 13 paragraph 5 e-Privacy Directive, after being amended by: Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Citizens' Rights Directive).
[132] Article 13 paragraphs 6 e-Privacy Directive, after being amended by the Citizens' Rights Directive.

Finally, this leads to the fourth point, namely that a number of countries have applied the rules of the Data Protection Directive itself to legal persons directly, by broadening the scope of the definition of 'personal data' and 'data subject'. It goes too far to discuss all those laws in detail, but reference can be made among others to Austria, where the concept of personal data also applies to legal persons. 'Personal Data' is defined as information relating to data subjects who are identified or identifiable. Data are only considered indirectly personal when the data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means. Importantly, a 'Data Subject' is defined as any natural or legal person or group of natural persons not identical with the controller, whose data are processed.[133] Likewise, some European countries not member to the EU have incorporated similar rules. For example the Swiss data protection act specifies: 'This Act applies to the processing of data pertaining to natural persons and legal persons by: a. private persons; b. federal bodies.'[134]

At this point, it is good to underline that certain of the first legislations (the Norwegian, the Luxemburgish, the Austrian and the Italian) had extended the protection directly to the legal persons: first they consider that in certain cases like civil society associations, the protection of the legal persons is a way to protect the privacy of the members and their individual liberties. Secondly because the informational power of big companies Vis à Vis small companies justifies the same protection for these small companies as for individuals. Another argument was the fact that the distinction between legal persons and physical persons create discrimination between retailers working as individuals and retailers having adopted a societal form.[135]

There seems, from the beginning of the data protection movement, to be a divide between countries that allow legal persons protection and those that do not. The French draft legislation from 1976, for example, linked data protection to the importance of 'due respect for private life, individual freedoms and public freedoms'[136] and the German legislation from 1977 specified in article 1 that the 'purpose of data protection is to ensure against the misuse of personal data during storage, communication, modification and erasure (data processing) and thereby to prevent harm to any personal interest that warrant protection.'[137] On the other hand, the draft Austrian data protection act from 1974 specified that personal data meant 'information, including personal identification marks, relating to a natural person or a juristic person or a "personal company" [handelsrechtliche Personengesellschaft] in the sense of commercial law, either identified or likely to be identifiable'[138] and the Danish draft bill on private registers from 1973 specified, regarding its field of application, that any 'systematic collection and registration of information on the financial conditions of persons, associations or undertakings, or of information on personal or private matters, which may reasonably be required not to be disclose publicly, may take place only in accordance with the provisions of this Act.'[139]

This division has remained, although some countries that originally extended their data protection rules to legal persons, such as Italy and Luxembourg, seem to have deleted

[133] <https://www.dsk.gv.at/DocView.axd?CobId=41936>.
[134] <http://www.admin.ch/ch/e/rs/2/235.1.en.pdf>.
[135] Thanks to anonymous Reviewer 3 for these points.
[136] Dammann, p. 56.
[137] Dammann, p. 72.
[138] Dammann, p. 11.
[139] Dannmann, p. 44.

this possibility from their national framework.[140] The other way around, some countries that have historically linked data protection rules to the protection of individual interests and informational self-determination, seem to have extended the data protection rules to legal persons. As an example, reference can be made to a case from Germany in which the Court stressed that the question whether an 'action is well founded, depends on the validity of Community legislation. If it appears that the Regulation (EC) No 259/2008 is invalid, there is no legal basis for the processing (§ 7 para 1 No. 1 HDSG) and the complaint must be upheld. The applicant can, as a legal person, also rely on the right of informational self-determination under Article 2 paragraph 1 in conjunction with Article 1, paragraph 1 of the Basic Law and article 14, paragraph 1 and Article 19 paragraph 3 of the Basic Law, insofar as it regards the protection against unlimited collection, storage, use or disclosure of identifying or identifiable data. The rules from the Hessian Data Protection Act are also applicable to legal persons, to the extent that a constitutionally protected right to informational self-determination is provided under Article 14 of the Basic Law, and they shall apply mutatis mutandis.'[141]

Reference can also be made to the Data Protection Directive's scope, which is connected to the protection of individuals with regard to the processing of personal data on the one hand and to the free movement of such data on the other. The Directive also specifies that 'Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection'.[142] Thus, on the one hand, the Directive aims at protecting persons against the unlawful processing of their personal data, but on the other hand, aims at facilitating a free and open European data market, in which personal data can be shared, transported over borders and exchanged without stifling rules and obligations. Thus, the interests of legal persons as data processors are also explicitly acknowledged by the Directive and are put on the same level as that of the individual to restrict data processing.

This also appears from the case law of the European Court of Justice,[143] for example in the case of *ASNEF and FECEMD v. Administración del estado*, which concerned one of the six grounds for legitimate data processing, namely Article 7 sub (f), which provides that

[140] See among others: <http://ec.europa.eu/justice/policies/privacy/docs/studies/legal_en.pdf>.

[141] VG Wiesbaden, Beschluss vom 27. Februar 2009, Az. 6 K 1045/08.WI. German text: 'Ob die Klage begründet ist, hängt zunächst von der Gültigkeit der vorgelegten Gemeinschaftsvorschriften ab. Erweist sich die Verordnung (EG) Nr. 259/2008 als ungültig, fehlt es an einer Rechtsgrundlage für die Verarbeitung (§ 7 Abs. 1 Nr. 1 HDSG) und der Klage ist stattzugeben. Die Klägerin kann sich als Gesellschaft ebenfalls auf das Recht der informationellen Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und Art. 14 Abs. 1 sowie Art. 19 Abs. 3 GG insoweit berufen, als ihren Trägern Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe der betreffenden individualisierte oder individualisierbarer Daten zusteht (vgl. BVerwG, Urteil vom 20.12.2001, Az.: 6 C 7/01, Rdnr. 18 - nach Juris; BVerfG, Beschluss vom 01.10.1987, Az.: 2 BvR 1178/86 u. a., Rdnr. 126 - nach Juris; BVerfG, Urteil vom 17.07.1984, Az.: 2 BvE 11/83, 2 BvE 15/83, Rdnr. 135 f. - nach Juris; VG Wiesbaden, Urteil vom 07.12.2007, Az.: 6 E 928/07, S. 11). Insoweit sind die Ausführungen des Hessischen Datenschutzgesetzes auch auf juristische Personen, soweit ein grundrechtlich verbürgtes Recht auf informationelle Selbstbestimmung nach Art. 14 GG gegeben ist, entsprechend anzuwenden.' This seems to be confirmed by: VG Wiesbaden, Urteil vom 18. Januar 2008, Az. 6 E 1559/06

[142] Article 1 Data Protection Directive.

[143] See also: Judgment of the Court (Third Chamber) of 30 May 2013. Worten - Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT). Case C-342/12. Judgment of the Court (Third Chamber) of 7 November 2013. Institut professional des agents immobilisers (IPI) v Geoffrey Englebert and Others. Case C-473/12. Judgement of the Court 20 May 2003. In Joined Cases C-465/00, C-138/01 and C-139/01, echnungshof (C-465/00) and Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG, and between Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) and Österreichischer Rundfunk.

data processing is legitimate when the interests of the data controller outweigh those of the data subject. This allows data controllers to process personal data of data subjects even without their consent. However, the Spanish implementation of this provision restricted to a large extent the possibility of balancing the interests, therewith providing extra protection to data subjects. The ECJ indicated that the Directive's Article 7 sub (f) has direct effect, that legal persons as data controllers can rely on it and that national implementation which further tighten the rules on data processing than does the Directive are invalid.[144]

Perhaps more importantly, the Court of Justice has in several cases explicitly acknowledged that legal persons may also rely on the material elements of the data protection rules for protection. Legal person, may, in the general interest, submit complaints about violations of data protection rules, such as the European Commission, when countries have incorrectly implemented the Directive in their national legislation,[145] the national Data Protection Authorities or the national Ombudsman.[146] But there are also cases in which businesses are allowed to rely directly on data protection rules for the protection of their own interests, such as Scarlet/Sabam and Promusicae. When an internet intermediary can be held liable for infringements of intellectual property of third parties by its users, but may equally be held liable if they reveal their users' identity or monitor their services, the Court has argued that the respective interests must be weighed against each other. Like with the rules on spam, internet providers can invoke the data protection rules to protect the interests of their users, but also to protect their own legitimate interests.[147]

The Working Party also argues that the European Court of Justice, in its *Lindqvist ruling*, explicitly allowed for such interpretations. 'The European Court of Justice has made clear that nothing prevents the Member States from extending the scope of the national legislation implementing the provisions of the Directive to areas not included within the scope thereof, provided that no other provision of community law precludes it. Accordingly some Member States such as Italy, Austria or Luxembourg have extended the application of certain provisions of national law adopted pursuant to the Directive (such as those on security measures) to the processing of data on legal persons. As in the case of information on dead people, practical arrangements by the data controller may also result in data on legal person being subject de facto to data protection rules. Where the data controller collects data on natural and legal persons indistinctly and includes them in the same sets of data, the design of the data processing mechanisms and the auditing system may be set up so as to comply with data protection rules. In fact, it may be easier for the controller to apply the data protection

[144] Judgment of the Court (Third Chamber) of 24 November 2011. Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Joined cases C-468/10 and C-469/10.Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado.

[145] Judgment of the Court (First Chamber) of 4 October 2001. - Commission of the European Communities v Grand Duchy of Luxemburg. - Failure by a Member State to fulfil its Treaty obligations - Non-incorporation of Directive 95/46/EC. - Case C-450/00. Judgment of the Court (Grand Chamber) of 9 March 2010 — European Commission v Federal Republic of Germany (Case C-518/07). Judgment of the Court (Grand Chamber) 9 March 2010 Case C-518/07 European Commission v Federal Republic of Germany. Judgment of the Court (Grand Chamber) of 8 April 2014. European Commission v Hungary. Case C-288/12.

[146] Judgment of the Court (Grand Chamber) of 16 December 2008. Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy. Case C-73/07.

[147] Judgment of the Court (Third Chamber) of 24 November 2011. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Case C-70/10. Judgment of the Court (Grand Chamber) of 29 January 2008. Productores de Música de España (Promusicae) v Telefónica de España SAU.Case C-275/06.

rules to all sorts of information in his files than to try to sort out what refers to natural and what to legal persons.'[148]

Consequently, under the Data Protection Directive, Member States are explicitly allowed to apply the data protection rules to legal persons and a number of European countries have done so. With the upcoming Regulation, which has direct effect and thus needs not be implemented in the different national laws of the Member States, it is unsure whether this possibility remains. A recital seems to explicitly discourage such interpretation: 'The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the legal person contains the names of one or more natural persons.'[149] Given the fact that, as the Working Party 29 signals, data regarding natural and legal persons are becoming more and more intertwined and less and less easy to disentangle, it remains to be seen what the new practice on this point will be. Still, it needs to be stressed that even if the Regulation itself could not be directly invoked by legal persons, states will presumably be at liberty to extent data protection rules to legal persons in their national legal framework.

3.3. The protection of legal persons' data protection concerns

As with privacy, however, it seems that, even when legal persons are allowed protection under data protection regimes, not all rights and freedoms are applied to them.[150] This finding is confirmed by a number of sources. For example, the Working Party 29 refers solely to the 'security measures' also applying to legal persons.[151] This relates to article 16 of the Data Protection Directive, specifying the principle of confidentiality of data processing, and article 17, specifying that the controller of personal data must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Consequently, legal persons may have legitimate interests in having data regarding them processed confidentially and safely.

Christopher Kuner, analyzing the systems of Austria, Denmark, Italy and Luxembourg and of non-EU members Liechtenstein and Switzerland also seems to signal a difference in protection. 'In some Member States, the courts have been reluctant to extend the same protection to data of legal entities that is granted to data of natural persons, even when national data protection law covers the personal data of legal persons. For example, in one case, the Austrian Federal Supreme Court (Oberster Gerichtshof) decided that a company processing data of its customers and suppliers for its own purposes is not a 'data subject' within the meaning of the Austrian Data Protection Act 2000, and so could not assert data

[148] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data', 01248/07/EN, WP 136, 20 June 2007, Brussels, p. 24.
[149] Recital 12 European Commission Proposal (2012).
[150] <https://www.dsk.gv.at/DocView.axd?CobId=41936>. <http://www.admin.ch/ch/e/rs/2/235.1.en.pdf>.
[151] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data', 01248/07/EN, WP 136, 20 June 2007, Brussels, p. 24.

protection claims against a competitor who was using such data.'[152] This is also reflected in the legislation of other countries granting protection to legal persons, as discussed by Kuner.

Finally, Douw Korff, who has done a study for the European Commission on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons, has concluded in similar spirit. He has, among others, differentiated between different situations and purposes of data processing and has stressed that those countries he analyzed which granted some protection to legal persons (Austria, Denmark, Iceland, Italy, Luxembourg, Norway and Switzerland) especially focused on data processing having an impact on the financial credibility of legal persons. 'Legal persons are clearly crucially affected by the processing of information on them, used to assess their creditworthiness or general business *bona fides*, or to "warn" potential customers. This is therefore, not surprisingly, the one area on which those countries which already apply data protection law to legal persons agree such protection should be retained. It might be noted, moreover, that in some countries (in particular, some Scandinavian countries) credit reference and business information services are very tightly controlled.'[153] Again, legal persons are not granted full and equal protection, but can only rely on a part of the data protection principles applied to natural persons.

Consequently, if businesses and other legal persons are allowed to directly invoke the data protection rules, they usually enjoy a limited form of protection only. Moreover, it seems very unlikely that legal persons would be allowed to invoke all new subjective rights accorded to natural persons under the Directive and especially the Regulation currently being under discussion. Like with the right to privacy, which has shifted from a doctrine principally regarding the obligation of states not to be subjected to arbitrary governmental interference to a subjective right of the natural person to flourish to the fullest extent and develop his personality to the maximum, the data protection rules have transferred from a doctrine specifying obligations for the data controller to process data fairly, correctly and adequately and be transparent about the data processing, to a right of the natural person, who may invoke a number of subjective rights, such as the right to be forgotten and data portability. As with the new rights developed and accepted under the doctrine of privacy (Article 8 ECHR), it seems very unlikely that these new data protection rights will be applied to legal persons, as they specifically aim to protect the individual interest of the natural person. Consequently, the divide between the protection of natural and legal persons will presumably only be deepened.

3.4. Conclusion section 3

Three points have been made in this section. First the material scope of the right to data protection has extended quite considerably. Data protection, originally, primarily entailed an obligation for states or other large data processors not to abuse their power, that is, not to gather data that are not necessary or proportionate to the goal pursued, storing data safely and confidentially, being transparent about the data processing, etc. It granted only marginal subjective rights to natural persons, such as to have access to personal data and to correct them. However, it has undergone a significant change. More emphasis has been placed on the protection of natural persons and their private interests, among others, by

[152] C. Kuner, 'European data protection law: corporate compliance and regulation', Oxford, Oxford University Press 2nd ed, 2007, p. 79. See: Oberste Gerichtshof, Decision of 4 May 2004, no 4 OB 50/04p.
[153] D. Korff, 'Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons, Commission of the European Communities, Study Contract ETD/97/B5-9500/78', p. 44-45. <http://ec.europa.eu/justice/policies/privacy/docs/studies/legal_en.pdf>.

giving them a number of subjective rights. Especially under the proposed Regulation, the individual will get a number of far-reaching rights, such as the right to be forgotten, the right to data portability and a right to object to profiling.

Second, traditionally, natural persons have been granted protection under the scope of the right to data protection. In more recent years, legal persons are increasingly allowed to invoke certain provisions. The protection of legal persons under data protection regulation has always been a matter of debate. In a way, some early definition leaves room for or explicitly acknowledges that legal persons also have a right to data protection. For example, Westin's definition of privacy in Privacy and Freedom is 'the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others'.[154] Institutions are of course legal persons. Similarly, from early on, certain national data protection laws have included legal persons under the concept of 'data subject', while others have rejected this interpretation.

In general, the concept of personal data has been more and more disconnected from the individual (natural person), and now includes, among others, identifiable information and indirect identifying information. This trend of a broadening material scope of data protection leaves more room for non-natural persons to invoke the right to data protection. Moreover, the e-Privacy Directive, *a lex specialis* of the Data Protection Directive for the electronic environment, explicitly aims at protecting the interest of legal persons. The General Data Protection Regulation, which will replace the Directive in time, will allow legal persons to submit a complaint on behalf of natural persons or in the interest of one of more natural persons. Finally, the Working Party 29 and others have explicitly argued for extending the rules from the Data Protection Directive to legal persons, among other things, because the difference between personal data and data relating to legal persons is not always clear.

Again, like with the rules on privacy, it seems that this entanglement of private and public, of personal and professional, of the interests of natural and legal persons, is partially due to the widening scope of the data protection rules. The extension of the scope of the concept of 'personal data' has meant that virtually all data may become personal data. Likewise, the individual has been granted more and broader rights, among others to control data, even if they are public or refer to professional information. Because the extension and because the professional life of a person may be part of his private life, data referring to his one man firm or his working life, may reveal a great deal about his identity and personae, and because his professional communications may also contain personal data, more and more, the data protection rules are extended to the public and professional sphere of the data subject. Thus, it has been argued that the strict separation between the protection of the natural person and the legal person is becoming more and more artificial.

Third and finally, legal persons are only allowed partial protection. Under most data protection regimes that do grant protection to legal persons, they may only rely on certain provisions, such as the protection against unfair treatment, access to data and the rules on processing data secure and confidentially. Like with privacy, data protection could be said to originally protect a societal value and not or only partially an individual value, related to fair and transparent data processing. Like with privacy, data protection has been focused more and more on the individual interest of natural persons, among others, by granting them subjective rights. In those regimes that allow legal persons to invoke data protection rules, it

[154] A. F. Westin, 'Privacy and freedom', London, The Bodley Head, 1970.

is likely that they may only rely on the general principles of fairness and transparency and not on the 'new rights', such as the right to be forgotten, the right to protection against profiling and the right to data portability. The next section will analyze whether this is a positive development and argue that a two-tiered system in the protection of data protection could be envisaged: one for data protection as a doctrine that (primarily) protects a societal value, one for data protection as a doctrine that (primarily) protects an individual value.

4. Analysis

The protection of the interests of legal persons is as such rather unproblematic. Data regarding them, too, should be processed confidentially and safely, kept correct and up to date and removed when no longer necessary. Similarly, if governmental officials enter business premises, confiscate business documents or wire-tap professional communications, this too should be done only when it is necessary, proportionate and effective and has a legal basis. It could be argued to the contrary that even though the interests of legal persons deserve protection, it should not be granted under the privacy and data protection regimes as those are installed to protect the individual and his personal interests. This article has suggested, however, that the background of both doctrines does not lie in the protection of natural persons and their individual interests. Rather, the underlying value was a societal interest and both originally primarily concerned the prohibition of abuse of power and principles of good governance. There seems no principled reason why legal persons should not fall under the scope of such doctrines.

Rather, it seems increasingly inevitable to open up protection for legal persons. Both with regard to classic privacy and data protection concerns, it is increasingly hard to differentiate between natural and legal person. As the ECtHR has considered, increasingly, companies are operating from premises also functioning as the home of a natural person and private and professional relations and conversations are more and more intertwined, among others, because of the growing number of one-man businesses. Similarly, data can be increasingly linked, combined and aggregated, so that even data originally only identifying a legal person, may, if linked to other data, be used to create a profile of a natural person. Sticking to the classic distinction between natural and legal persons in this environment seems to be unpractical and would have as outcome that some valuable interests would be denied an adequate level of protection. Finally, reference can also be made to the risk of discrimination between a merchant operating on an individual basis and the same merchant operating under the coverage of a legal person.

To the contrary, it may be argued that broadening the scope of privacy and data protection regimes would result in considerable extra effort, costs and court proceedings. It is however questionable whether this is truly so. Presumably most states and data processers will already apply some protection to legal persons, given the point made in the previous paragraph, and it will entail limited extra effort and costs to extent the level of protection to legal persons. Rather, it could be argued that in the future, given the technological developments, it would entail more effort and costs to keep a strict separation between the two types of persons than simply apply a (minimum) level of protection to both. It is also questionable whether this extended scope will result in a much higher number of cases. Under the European Convention, since the Court has opened up complaints under Article 8 ECHR for legal persons in 2002, only a couple cases submitted by legal persons seem to have been treated by the Court, compared to the more than 1000 cases filed by individuals.

Still, a difference between natural and legal persons should be maintained. Although it seems rather unproblematic to, as a principle, extent the protection of both regimes to legal persons (this would include the current Regulation being under discussion), they should not be able to enjoy a similar level of protection. Rather, a two-tiered system should be introduced.[155] First, many of the 'traditional' obligations for states and data controllers could without problem be transposed to legal persons, though not all. For example, the protection of family life seems hard to apply to businesses. Although it could be argued that this may be compared to businesses being able to install a daughter or sister company, this seems to be too far removed from the traditional sphere of the right to privacy, among other reasons, because this may include a positive freedom instead of a negative freedom.[156] Similarly, some traditional data protection principles seem difficult to apply to legal persons, for example, the extra protection provided to sensitive data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.[157] Again, would this be transferred in analogy to legal persons, it would regard something like the protection of business secrets, which seems at odds with the background of data protection, as it principally aims at protecting economic concerns. Other principles, such as the notification requirement, the principles on fair and legitimate data processing, the obligation to keep data correct and update and process them safely and secure seem however quite easily applicable to legal persons and their interests.

The previous paragraph concerned the obligations for states and data processers to use their power in a fair and legitimate way, which can in principle be transposed to legal persons. With regard to the subjective rights granted under both regimes, the application to legal persons seems to be more problematic, though some might be. Why, for example, should they not have the right to access information processed regarding them or to request alteration when they are incorrect, incomplete or not up to date? Rights to be forgotten and data portability, inter alia, seem however less easy applicable to legal persons. They are of more recent origin and take as principle concern the protection of the individual and his personal interests. The same can be said about the new rights and freedoms developed under Article 8 ECHR, such as the right to respect for minority cultures.

Finally, a difference could be introduced between the level of protection, similar to the protection of the freedom of speech, with regard to which a difference is often made between commercial and political speech, the former enjoying a lower standard of protection than the latter, because the first serves a value (commercial interest) commonly regarded as inferior to the second (free political debate as precondition of a democratic state).[158] It seems that a similar distinction can be made with regard to privacy and data protection doctrines, though not in the underlying value. With a prohibition, for example, of governmental officials to enter business premises without good reason and legal safeguards, it is not the commercial interest of the company as such that is at stake, but the legitimacy of the state and governmental organizations, among others in relation to the prohibition on the abuse of

[155] See also: M. Emberland, 'The Human Rights of Companies: Exploring the Structure of ECHR Protection', Oxford, Oxford University Press, 2006.
[156] Perhaps it could be argued that a right to respect the relationship between already established mother and daughter companies could be compared with a negative obligation, but this seems to regard the protection of economic interests.
[157] Article 8 Data Protection Directive.
[158] See also for this suggestion the works of Emberland. See further on this topic: E. Barendt, 'Freedom of speech', Oxford, Oxford University Press, 2005.

power. Although the underlying value and concern is the same, it is undeniable that there is a difference in the effects, as the entering of homes of natural persons may have a large impact on the lives of natural persons, while the effects of entering business premises merely entails a hindrance and nuisance to the business activities. Consequently, with regard to the level of protection and especially the amount of compensation payment afforded to a victim of a privacy or data protection violation, a difference could be made between the level of protection offered to legal and natural persons.

Thus, two systems of protection could arise. First, the traditional doctrines of privacy and data protection that concern principles of good governance, duties of care and a prohibition on the abuse of power could be applied to natural and legal persons alike. Exceptions are possible, for example in relation to the protection of 'family life' and 'sensitive data', which are hard to transpose to legal persons. The new rights and freedoms, specifically installed to protect the individual's personality and the capacity to develop and flourish to the fullest extent, shall only be applied to natural persons. Some marginal rights, such as in relation to accessing and correcting data, might also be applied to legal persons. Finally, a difference should be made in the level of protection and compensation offered to natural and legal persons in case of a violation.

Two-tiered system for privacy and data protection	**Natural Persons**	**Legal Persons**
Negative obligations for states and data controllers	Full protection	Similar protection, with some exceptions such as the right to family life and the protection of sensitive data
Positive rights for persons and data subjects	Full protection	In principle, no positive rights, perhaps with the exception of the right to access and alteration of data
Level of protection offered	Full protection	Lower level of protection and lower level of compensation for violations

With regard to the right to privacy, provided under Article 8 ECHR, no substantial revisions are required to implement such a system. The European Court of Human Rights already allows legal persons to invoke this right, albeit the number of cases has been limited. Article 8 ECHR provides protection to the private life and family life, home and communications. The Court has already limited its rulings with regard to legal persons to violations of their business premises (home) and communication and has never extended the protection of private life and family life to legal persons. Likewise, so far, it has never allowed legal persons to invoke the 'new' positive rights, such as have been granted under the right to privacy in the Convention. Article 34 of the ECHR already provides for complaints by legal persons, as it specifies that the Court may receive applications from 'any person,

nongovernmental organisation or group of individuals' claiming to be the victim of a violation of the rights set forth in the Convention.

Likewise, the Convention seems to allow for a differentiation between the compensation granted to natural persons and legal persons. Article 41 provides that if the Court finds that there has been a violation, and if the internal law of the state concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party. The Rules of the Court[159] clarify that a differentiation can be made between (a) pecuniary damage; (b) non-pecuniary damage; and (c) costs and expenses. Obviously, both natural persons and legal persons can claim satisfaction for costs and expenses. Likewise, pecuniary damage may be awarded to both parties. However, legal persons should not be able to invoke compensation for non-pecuniary damages. The Rules of the Court specify that the 'Court's award in respect of non-pecuniary damage is intended to provide financial compensation for non-material harm, for example mental or physical suffering.'[160] Obviously, legal persons cannot suffer mental or physical harm, while for natural persons it seems especially this form of non-pecuniary harm that is applicable to privacy violations. A house search, for example, does not so much cause for material damage as for emotional stress; placing children out of home hampers the family life, but has little or no financial impact.

Businesses should be allowed to request compensation for pecuniary damages. The rules of the Court specify: 'The principle with regard to pecuniary damage is that the applicant should be placed, as far as possible, in the position in which he or she would have been had the violation found not taken place, in other words, *restitutio in integrum*. This can involve compensation for both loss actually suffered (*damnum emergens*) and loss, or diminished gain, to be expected in the future (*lucrum cessans*). It is for the applicant to show that pecuniary damage has resulted from the violation or violations alleged. The applicant should submit relevant documents to prove, as far as possible, not only the existence but also the amount or value of the damage.'[161] Still, it must be stressed that the financial damage suffered from an 'ordinary' privacy violation, for example, wire-tapping businesses communication, is close to nil.

At most, businesses may suffer in reputation (which might affect their profitability) if police investigations, wire-tapping and searches of business premises are made public. In these cases, the legal person would need to demonstrate the causal relationship between the reputational damage and the financial loss. In other cases, they will not be awarded financial compensation, but the state may be reprimanded by the ECtHR for a privacy violation. Possibly, a cease and desist order may be imposed which, if violated, may lead to a sanction. More importantly, it might be worthwhile considering the introduction of the possibility of a fine or penalty, independent of financial compensation for victims of a privacy violation.

With regard to the data protection rules, some changes may be necessary. The Regulation could specify that it also aims at protecting the interests of legal persons, or even better, at protecting societal interests, relating to safe, fair and legitimate data processing, which apply to natural and legal persons irrespectively. Right now, the Regulation specifies that it lays down rules relating to the protection of individuals with regard to the processing

[159] <http://www.echr.coe.int/Documents/Rules_Court_ENG.pdf>.
[160] <http://www.echr.coe.int/Documents/Rules_Court_ENG.pdf>.
[161] <http://www.echr.coe.int/Documents/Rules_Court_ENG.pdf>.

of personal data and rules relating to the free movement of personal data.[162] Besides the subject matter and aims of the Regulation, an alteration could be made to the scope. Right now, the data subject is defined as 'an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.' The Regulation could simply specify that a data subject is 'an identified natural or legal person or a natural or legal person who can….' or just refer to 'person'.

With regard to the protection of legal persons, a differentiation could be made between the several chapters in the Regulation. There are a number of rules which lay down obligations for data processors, which could easily be separated from the interests of the data subject. Chapter IV, titled Controller and Processor, contains rules specifying the duties and responsibilities of the data controller, such as to keep documentation on the data processing,[163] implementing data security requirements,[164] performing a data protection impact assessment,[165] complying with the requirements for prior authorization or prior consultation of the supervisory authority[166] and designating a data protection officer.[167] The data controllers should comply with these rules, independently of whether they process data of natural persons, legal persons or both.

Chapters II, titled Principles, and III, titled Rights of the Data Subject, both contain rules which could be applied to both natural and legal persons and rules which should only be applied to natural persons. In Chapter II, article 5 specifies the principles relating to personal data processing, such as that personal data must be processed lawfully, fairly and in a transparent manner; collected for specified, explicit and legitimate purposes; must be adequate, relevant and limited to the minimum necessary; accurate and kept up to date; and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. These rules should be applicable to both natural and legal persons. This also holds true for Article 6, which specifies six grounds (much like the Directive) for legitimate data processing, such as consent, the performance of a contract, compliance with a legal obligation and when the interests of the data controller outweigh those of the data subject.

However, Article 9 specifies grounds for legitimately processing sensitive data, such as data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited. Obviously, legal persons do not have such sensitive data and this provision should not be applicable to them. This also holds true for Article 8, containing rules on the processing of personal data of a child, and Article 7 containing conditions for consent. This last article provides, among other things, that the controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. This article is aimed at protecting natural persons, which are presumed the weaker party in relation to, for example, larger

[162] Article 1 European Commission Proposal (2012).
[163] Article 28 European Commission Proposal (2012).
[164] Article 30 European Commission Proposal (2012).
[165] Article 33 European Commission Proposal (2012).
[166] Article 34 European Commission Proposal (2012).
[167] Article 35 European Commission Proposal (2012).

companies such as Google and Facebook; the same ratio, however, does not apply to legal persons, or to a lesser extent.[168]

Likewise, Chapter III contains some provisions which could be applied to legal persons and others that should not. The rules on transparency and the right to access could be applied to the processing of data of legal persons. Article 11 provides that the controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. Article 14 provides, inter alia, that where personal data relating to a data subject are collected, the controller shall provide the data subject with at least information about the identity and the contact details of the controller; the purposes of the processing for which the personal data are intended; the period for which the personal data will be stored; and the recipients or categories of recipients of the personal data. The controller should respect these provisions, irrespectively of whether he is processing person data of natural persons, legal persons or both. Perhaps, this should also count for the right of access, provided in Article 15, which grants the data subject a right to know, among other things, the purpose of the processing, the categories of personal data, the recipients or categories of recipients to whom the personal data are disclosed, the period for which the personal data will be stored, etc. Likewise, the right to rectification, laid down in Article 16, providing that the data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate, could be applied to legal persons.

These provisions all regard general interests, such as that data processing should be done fairly and transparently and that the data should be accurate and kept up to date. However, certain subjective rights, such as the right to data portability (Article 18), the right to be forgotten (Article 17) and the right to object to profiling (article 20) should only be applied to natural persons. These articles provide natural persons with a right to control or even own their personal data, to protect persons, especially minors, from the fear of being stigmatized and burdened by a piece of information the rest of their lives and to protect natural persons from being profiled, especially on the basis of sensitive information. Such concerns are and should not be applicable to legal person.

Finally, a question remains with regard to the level of compensation. A difference can be made between sanctions and the right to compensation. The Regulation introduces a tripartite system for administrative sanctions in Article 79. One regime in which the supervisory authority may impose a fine of up to 250,000 euro, or in case of an enterprise up to 0.5 per cent of its annual worldwide turnover, the second involves a fine of up to 500,000 euro or 1 per cent of the annual worldwide turnover, and the third a fine of up to 1,000,000 euro or 2 per cent of the annual worldwide turnover. The first is applied to instances in which the data controller has disrespected the principles on transparency; the second regards, among other things, a violation of the individual's right to information, access to personal data, the right to rectification, the right to be forgotten, and the right to data portability; and the third applies, among other aspects, to instances in which the principles on the processing of sensitive personal information have not been respected, the principles concerning consent have been violated, or the personal data of a child have been processed without the agreement of the parent, the right to object and the right to protection against profiling have been violated, the accountability duty has been disrespected, or personal data have been processed

[168] Perhaps, reference could be made to the 'weaker' position of small businesses in relation to large companies in B2B relations.

unlawfully. As a sanction is not directly connected to the interests of the data subject, but to the respect by the data controller for the obligations the Regulation lays down, there seems no reason why this system could not also be applied to the situation of legal persons.

With regard to the right to compensation, like with the right to privacy, the amount of damage legal persons may be compensated for must be limited to pecuniary damages (and the costs and expenses for the legal proceedings). The Regulation seems to allow for sufficient flexibility in this respect. Article 77 provides that any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered. So, in conclusion, no fundamental alteration to the Regulation is necessary in respect of the possibility to impose sanctions or to beget financial compensation for damage suffered. These rules are applicable to both natural and legal persons.

Acknowledgement

Bart van der Sloot is a researcher and coordinator of the Amsterdam Platform for Privacy Research (APPR). This research is part of a project 'Privacy as virtue' funded by Netherlands Organisation for Scientific Research (NWO) (http://www.nwo.nl/en/research-and-results/research-projects/04/2300172004.html). Project number is: 406-11-119.