Centre for Information Policy Leadership
Hunton Andrews Kurth

9 November 2018

The ePrivacy Regulation and the EU Charter of Fundamental Rights

ABSTRACT/EXECUTIVE SUMMARY

An important focus in the legislative discussions on the proposed ePrivacy Regulation is the fact that the proposal (mainly the articles 5 and 6 thereof) aims to protect the confidentiality of communications of individuals and legal persons, and in particular addresses the confidentiality of content data and metadata, implementing Article 7 of the EU Fundamental Rights Charter ("right to privacy"). In contrast, the GDPR implements Article 8 of the Charter ("right to data protection").

The attached legal note argues that the difference between Articles 7 and 8 of the Charter has limited relevance, in connection to the ePrivacy Regulation.

It aims to demonstrate that EU law and in particular the Charter does not preclude a risk based approach, nor the processing of content data and metadata on the basis of legitimate interest, provided that the necessary safeguards protecting the individuals' communications are put in place. Neither Article 7 nor Article 52.1 of the Charter enumerate the grounds for limitation of fundamental rights. They do not prescribe that the right to privacy can be limited only on the basis of particular justificatory grounds, such as consent of the user.

The note also addresses a few connecting issues, such as the sensitive nature of content data and metadata, as well as the robust protection of individuals provided by the GDPR if an organisation relies on legitimate interests as a legal basis for processing electronic communications data, due to the increased accountability measures organisations need to take.

The note also deals with the confidentiality of communications of legal persons and explains that this confidentiality is not a matter of privacy and is protected under other EU law provisions.

Centre for Information Policy Leadership
Hunton Andrews Kurth

9 November 2018

The ePrivacy Regulation and the EU Charter of Fundamental Rights

This legal note on some key aspects of the proposed ePrivacy Regulation in the context of the Charter and the GDPR was written for the Centre for Information Policy Leadership by Maja Brkan, Assistant Professor of EU law at Maastricht University, David Dumont, Counsel at Hunton Andrews Kurth, and Hielke Hijmans, CIPL's Senior Policy Advisor.

INTRODUCTION

An important focus in the legislative discussions on the proposed ePrivacy Regulation (ePR)[1] is the fact that the proposal (mainly the articles 5 and 6 thereof) aims to protect the confidentiality of communications, and in particular addresses the confidentiality of content data and metadata.

As explained by the Explanatory Memorandum , the proposal serves to implement Article 7 of the EU Fundamental Rights Charter (the "Charter"). In contrast, the GDPR is about the protection of personal data, implementing Article 8 of the Charter (and the equivalent Article 16 TFEU). Recently, the European Data Protection Supervisor (EDPS) reiterated that the data protection reform would not be complete without the ePR, because the GDPR only concerns Article 8 of the Charter[2] (hence, not Article 7).

This note has a legal nature and will not discuss this policy statement of the EDPS. However, it will discuss a related argument.

As we understood, it is argued that the particular nature of ePR – protecting the right to privacy and communications – would preclude including a risk based approach as well as processing of content data and metadata on the basis of legitimate interest. These are important elements of fair and accountable data processing within the GDPR.

This note assesses this line of argument more in detail. It aims to demonstrate that EU law and in particular the Charter does not preclude a risk based approach, nor the processing of content data and metadata on the basis of legitimate interest, provided that the necessary safeguards protecting the individuals' communications are put in place.

[1] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM (2017) 10 final. We are aware that a number of amended versions is discussed in the legislative procedure in the EP and the Council. These amended versions are not separately discussed in this note.

[2] https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en

Centre for Information Policy Leadership
Hunton Andrews Kurth

TEN KEY POINTS

1. Articles 7 (right to privacy) and 8 (right to data protection) of the Charter are closely related; there are different views on how to construe this relationship. The Commission proposal for the ePR is based on the view that one of the elements of the right to privacy (Article 7) is a right to confidentiality of communications with a wide scope, including non-personal data.

2. The difference between Articles 7 and 8 of the Charter in connection to the ePR has limited relevance.

3. In so far as ePR gives expression to the right to privacy (Article 7 of the Charter), potential limitations of this right to privacy in the ePR should respect Article 52.1 of the Charter.

4. Neither Article 7 nor Article 52.1 of the Charter enumerate the grounds for limitation of fundamental rights. They do not prescribe that the right to privacy can be limited only on the basis of particular justificatory grounds, such as consent of the user. The legislator may limit this fundamental right for other reasons such as the legitimate interest of the provider of electronic communications, or justified interests of society.

5. Effective remedies for individuals must always be provided and safeguarded.

6. The Court of Justice specified the particularly sensitive nature of content data and metadata, although these data are not included in Article 9 of the GDPR on specific categories of personal data which cannot be processed on the basis of the legitimate interest of the controller.

7. Legal persons are entitled to invoke the confidentiality of communications, an element of Article 7 of the Charter. The protection can be safeguarded also on the basis of other EU instruments, such as the Directive on the Protection of Trade Secrets (outside of the scope of Article 7 of the Charter). Legal persons are not entitled to invoke Article 8 of the Charter.

8. The GDPR sets forth a robust set of rules, safeguards and limitations that must be respected by organizations when processing personal data and provides for effective remedies for individuals to enforce these. The GDPR will apply to almost any processing of electronic communications data.

9. The GDPR requires organizations that process electronic communications data to put in place robust security and confidentiality measures. The accountability and risk-based approach is the core of the GDPR (Article 24). It will result in organisations having to implement heightened protection, safeguarding measures and DPIAs, to reflect that processing of this type of data may result in high risks to individuals rights and freedoms.

10. Individuals' privacy rights actually may benefit from a strong protection if an organization relies on legitimate interests as a legal basis for processing electronic communications data, due to the increased accountability measures organisations need to take.

SECTION 1. THE DIFFERENCE BETWEEN ARTICLES 7 AND 8 OF THE CHARTER.

Article 7 of the Charter protects the respect for private and family life, home and communications. The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the European Convention of Human Rights (ECHR; 1950). To take account of developments in technology the word 'correspondence' in the Convention has been replaced by 'communications'.[3]

In the present context, we focus on the privacy of communications or, a bit wider, on "informational privacy." Privacy is a wide notion. It encompasses the "right to establish and develop relationships with other human beings" and does not exclude professional or business activities.[4]

Article 8 of the Charter lays down a fundamental right to the protection of personal data.[5] It is inspired by the main elements of the EU rules on data protection, such as those laid down in Directive 95/46, the predecessor of the GDPR. Article 8 of the Charter is also inspired by Article 8 of the ECHR (on the right to private life) and the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108).[6]

Articles 7 and 8 are closely related – the fact that they both connect to Article 8 ECHR is just an example – and the EU Court of Justice usually takes both articles together, when it scrutinizes EU data protection law. The landmark rulings of the Court in this domain – mainly *Digital Rights Ireland* (2014)[7] and *Schrems* (2015)[8] - illustrate this.

Two closely related rights

Also the legal doctrine confirms that both articles of the Charter are closely related, although there are different views on how to construe this relationship.

A first view is that on the internet and in particular in the era of big data, all processing of personal data potentially affects privacy and that privacy and data protection are two sides of the same coin. The right to privacy represents a normative value and the right to data protection the "rules of the game".[9] As said, the Court of Justice seems to take a similar approach. In this approach, data protection is in the first place a subset of privacy.

---

[3] See Explanations Relating to the Charter, OJ C 2007, 303/17.
[4] ECtHR, Case *Niemietz v Germany*, 1992, Application No. 13710/88, a explained by Jens Vedsted-Hansen in Steve Peers et al. (eds), *The EU Charter of Fundamental Rights. A Commentary* (Hart 2014), at 156-157.
[5] The Explanations Relating to the Charter explain the origin of Article 8 Charter.
[6] This Convention of 108 is in a process of modernisation. A new convention was recently adopted and is now open for signature. It will enter into force in the coming years.
[7] Joined cases C-293/12 and C-594/12, *Digital Rights Ireland* (C-293/12) *and Seitlinger* (C-594/12), ECLI:EU:C:2014:238.
[8] Case C-362/14, *Schrems*, ECLI:EU:C:2015:650.
[9] Hielke Hijmans, The European Union as Guardian of Internet Privacy, Springer 2016, at 2.8 and 2.12.

A second view emphasizes the distinctions between the rights. It is argued that the right to data protection serves a multitude of purposes; privacy is only one of them.[10] In other words, the right to data protection has a wider scope than the right to privacy. Others defend that the right to privacy offers additional protection for data that is not only personal, but also private.[11]

A third view focuses on the elements of the right to privacy.[12] One of the elements is a right to confidentiality of communications. This is the modern version of the old secrecy of letters precluding state authorities from opening envelops and reading letters. This right to confidentiality has a wide scope and exists independently of the content of communications, or, in other words, whether a communication contains personal data.

The latter is also the line of argument the Commission seems to defend in connection to the ePR. As the Commission explains in the Explanatory Memorandum, the proposal "implements in the Union's secondary law the fundamental right to the respect for private life, with regard to communications, as enshrined in Article 7 of the Charter of Fundamental Rights of the European Union". This is different from the GDPR, which implements Article 8 of the Charter (data protection).

The distinction between Art 7 and 8 of the Charter in connection to the ePrivacy Regulation has limited relevance

According to the doctrine, Articles 7 and 8 of the Charter are closely related, but they do not necessarily overlap. There may be a theoretical distinction, but this distinction has limited practical relevance, in any event in so far as these provisions are used as underlying justifications for the ePR and the GDPR.

First, the distinction in basis is not clearly cut. On the one hand, as we have seen above, according to the Explanatory Memorandum, the ePR implements Article 7 of the Charter. On the other hand, however, the ePR also implements Article 16 TFEU on data protection. The same Explanatory Memorandum explains that Article 16 TFEU is the main legal basis of the ePR.[13] Only because "*the proposal aims at protecting communications and related legitimate interests of legal persons*" (so, outside the scope of personal data protection) an additional

[10] Orla Lynskey, The Foundations of EU Data Protection Law, Oxford University Press 2015, at 90. See also Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer 2014, at 8.3.

[11] Christopher Docksey, Four fundamental rights: finding the balance, International Data Privacy Law, 2016, Vol. 6, No. 3, at 201. See further: Maria Tzanou, 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right', (2013) 3 International Data Privacy Law 2, 88–99; Aidan Forde, The Conceptual Relationship between Privacy and Data Protection, (2016) Cambridge L. Rev. 1, 135-149; Maja Brkan, 'The Court of Justice of the EU, privacy and data protection: Judge-made law as a leitmotif in fundamental rights protection' in Maja Brkan and Evangelia Psychogiopoulou (eds), Courts, Privacy and Data Protection in the Digital Environment (Edward Elgar 2017) 13-17.

[12] As further explained in Section 2 below.

[13] The legal basis of the instrument needs to be identified in order to ensure that the EU has legislative competence.

legal basis is needed.[14] Article 1 of the ePR on the subject matter mentions private life, communications and data protection together. Moreover, also the GDPR itself (Article 95 and recital 173) underlines that the ePrivacy regime contains "specific obligations with the same objective", meaning data protection.

Second, the object of the ePR may be different from that of the GDPR, but this seems mainly a matter of difference in wording. Whereas the GDPR applies to the processing of personal data, the ePR applies to the processing of electronic communications data (see Art 2 thereof). These are mostly personal data. However, Article 5 of the ePR safeguards the confidentiality of communications, which may – as explained above - be seen as something different from data protection. Therefore, the ePR does not deal with data subjects, controllers and processors, but with users and providers of an electronic communications service. The question however is: is this all not purely a matter of terminology?[15]

Third, Article 7 of the Charter has a wide scope (private life includes all kinds of communications with others) and also the notion of personal data has a wide scope: any information relating to an identified or identifiable natural person. In practice, there will not be much difference in scope.

There is one exception: communications data that do not relate to individuals but to legal persons. At this specific point, the ePR has a wider scope. Legal persons are entitled to confidential communications. But one can argue whether this protection of legal persons reflects privacy, as an expression of human dignity (see further Section 2).

- **Articles 7 (right to privacy) and 8 (right to data protection) of the Charter are closely related; there are different views on how to construe this relationship. The Commission proposal for the ePR is based on the view that one of the elements of the right to privacy (Article 7) is a right to confidentiality of communications with a wide scope, including non-personal data.**
- **The difference between Articles 7 and 8 of the Charter in connection to the ePR has limited relevance.**

[14] This additional legal basis is Article 114 TFEU.
[15] Apart from communications data of legal persons, discussed later in this note.

SECTION 2. RESTRICTIONS AND LIMITATIONS OF THE ENJOYMENT OF FUNDAMENTAL RIGHTS: WHAT IS ALLOWED BY ART 52.1 OF THE CHARTER?

The ePR gives expression to the fundamental right to privacy as enshrined in Article 7 of the Charter. In addition, the ePR gives expression to the fundamental right to protection of personal data from Article 8 of the Charter. The implementation of these two fundamental rights by the ePR is pointed out by the Commission in the Explanatory Memorandum to this Regulation[16] and is reflected in Article 1(1) of the ePR.

The notion of 'giving expression' is known from the fundamental rights case law, notably the *Kücükdeveci* case, and has since been also addressed in the doctrine.[17] The ePR therefore lays down concrete rules for implementation of this fundamental right.

The ePR will be directly applicable, also in the relationship between private companies and individuals, and can hence create obligations for the private sector.

From a constitutional point of view, such 'giving expression' is relevant because it means that potential limitations of the right to privacy that are laid down by the ePR need to inherently respect Article 52.1 of the Charter. That means that the EU legislator, before enacting these limitations, has to conduct a proportionality analysis and verify whether the limitations respect the essence of fundamental rights. Since the secondary legislation needs to inherently respect fundamental rights, the limitations of fundamental rights that are present in this secondary legislation should already be proportionate and respect the essence *ex ante*, before the legislation is enacted.

However, the Court of Justice of the EU can exercise an *ex post* control of compliance with proportionality and the essence which can lead to an annulment of secondary legislation as in *Digital Rights Ireland* and *Schrems*.

Limitations of fundamental rights, in particular Article 7 of the Charter

The rules on limitations of fundamental rights from the Charter, including potential limitations to the confidentiality of communications from its Article 7, are laid down in Article 52.1 of the Charter, which reads as follows: "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations*

[16] The Commission does not use these exact words, but rather specifies that the proposed Regulation "aims to make more effective and increase the level of protection of privacy and personal data processed in relation with electronic communications in accordance with Articles 7 and 8 of the Charter"; see Explanatory Memorandum to the proposal of the ePrivacy Regulation, point 3.6.

[17] More precisely on the notion of secondary legislation 'giving expression' to the principle of non-discrimination on grounds of age, see Case C-555/07, *Kücükdeveci*, ECLI:EU:C:2010:21, paras 21, 27, 32, 43, 50, 51, 53, 55, 56. Compare Elise Muir, The Fundamental Rights Implications of EU Legislation: Some Constitutional Challenges, 51 Common Market Law Review, 219-245 (2014), who confirms, at 232, that the EU secondary legislation in the field of data protection gives expression to the fundamental right to data protection. Compare also Orla Lynskey, The Foundations of EU Data Protection Law, Oxford University Press 2015, at 36.

may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

The wording of this provision implies that the compatibility of a limitation of fundamental rights to privacy (Article 7) and data protection (Article 8) needs to be assessed in several steps: first, the limitation needs to be laid down by law; secondly, the limitation needs to respect the essence of the fundamental right and third (if the essence of this fundamental right is respected), the limitation needs to respect the principle of proportionality. It is arguable in the doctrine as well as in the case law of the CJEU whether the second and third step are mutually exclusive.[18]

In practice, if essence and proportionality are to be seen as two separate concepts, then the courts, when assessing compliance of a measure with the Charter, should first verify whether a measure impairs the essence of this fundamental right.[19] If it does, the analysis stops there and there is no need to verify whether the measure is proportionate. The proportionality analysis would become relevant only in the next step, after determination that the measure respects the essence of this fundamental right.

The issue of the respect of essence of fundamental rights raised an interest especially after the *Schrems* case, the first case in which the CJEU found that there was an impairment of essence of fundamental rights to privacy (Article 7 of the Charter) and to effective judicial protection (Article 47 of the Charter).

With regard to the right to privacy, the Court in *Schrems* seems to further develop the argument from *Digital Rights Ireland*, according to which the essence of privacy is impaired if a measure in question allows for 'the acquisition of knowledge of the content of the electronic communications'.[20]

In *Schrems*, the Court confirmed this argument by stating that the legislation permitting '*the public authorities to have access on a generalised basis to the content of electronic communications*' does not respect the essence of the fundamental right to privacy from Article 7 of the Charter. The relationship between the access to content of electronic communication and the impairment of essence of this fundamental right was further confirmed in the *Tele2 Sverige* case where the Court, in the absence of access to such content, did not find an impairment of essence of this right.[21]

Turning from the concept of essence to the justification of interference and the principle of proportionality, the latter analysis, according to the case law of the CJEU encompasses two steps. After determination that the interference has been provided by law, it first needs to

[18] See Maja Brkan, The concept of essence of fundamental rights in the EU legal order: peeling the onion to its core, 14 European Constitutional Law Review (2018) 336-337.
[19] Compare *ibid*., 360.
[20] See *Digital Rights Ireland,* para 39, where the CJEU confirms that the controversial Data Retention Directive does not adversely affect the essence of the fundamental right to privacy as it does not allow for 'the acquisition of knowledge of the content of the electronic communications'.
[21] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson*, ECLI:EU:C:2016:572, para 101.

be established whether the interference can be justified with an objective of general interest.[22] The second step, proportionality analysis, further encompasses two steps: appropriateness and necessity of the measure.[23]

Turning to the argument that Article 7 of the Charter can be limited only in cases of consent of the user of electronic communications, it needs to be pointed out that neither Article 7 nor Article 52.1 of the Charter enumerate the grounds for limitation of fundamental rights. In other words, Article 52.1 of the Charter is a general clause which does not restrain potential grounds for limitation of fundamental rights. If a justificatory ground pursues an objective of general interest, the CJEU will accept it as a potential justification and verify whether the limitation of the fundamental right is proportionate with that general interest.

As a consequence:

a) Neither Article 7 nor Article 52.1 of the Charter prescribe that a particular fundamental right, in this case the right to respect for private life, can be limited only on the basis of particular justificatory grounds, such as consent of the user.

b) The legislator may decide to limit this fundamental right for other reasons in the general interest. Among those reasons can be, for example, rights and freedoms of others (such as the legitimate interest of the provider of electronic communications), public health, public security,[24] preventing of serious crime and others. As the recent case *Ministerio Fiscal* demonstrates, preventing of serious crime can be a justificatory ground for a limitation of Articles 7 and 8 of the Charter, within the framework of the interpretation of the ePrivacy Directive currently in force.[25]

Importance of remedies for privacy and data protection

Schrems case attests to the importance of remedies for effective enforcement of Articles 7 and 8. In this case, the CJEU went as far as to recognise that the complete absence of legal remedies to obtain access to personal data or rectification or erasure of such data, amounts to the impairment of essence of the fundamental right to effective judicial protection from Article 47 of the Charter.[26]

If this finding is extrapolated to other fundamental rights, a more general claim can be made that an absence of legal remedies for enforcement of rights will by definition lead to an interference with the said Article 47. Whether such absence of remedies could potentially and exceptionally be justified in a particular case would depend on individual circumstances

[22] See for example *Digital Rights Ireland*, para 41.
[23] See for example *Digital Rights Ireland*, para 46, and the case law cited there.
[24] Note, however, that *national* security, in accordance with Article 4 TEU, 'remains the sole responsibility of each Member State'. The exact scope of this notion and the distinction with the wider notion of public security exceeds the scope of this legal note.
[25] *Ministerio Fiscal*, Case C-207/16, ECLI:EU:C:2018:788, para 63.
[26] *Schrems*, para 95.

of a case, but in principle fundamental rights should have an effective enforcement apparatus attached to them.

The Court in *Schrems* further stresses that 'everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal',[27] further stressing the importance of remedies in fundamental right enforcement.

Fundamental rights implications of distinction between content and metadata

As mentioned above, the CJEU recognised, in its case-law such as *Digital Rights Ireland*, *Schrems* and *Tele2 Sverige*, that unlawful processing of both content data and metadata can lead to an interference with both Articles 7 and 8 of the Charter. However, while the Court recognised that the *interference* with these fundamental rights can be due by the access to both content data and metadata, the constitutional *reasoning* as to how to reach this conclusion seems to differ depending on the type of data involved.

The case law of the Court seems to imply that the generalised access by public authorities to content data leads to an impairment of *essence* of the fundamental right to private life (*Schrems*[28]), whereas access to metadata leads to an unjustified *disproportionate* interference with this right (in that sense, *Tele2 Sverige*[29]). Given that the distinction in seriousness of access to metadata and content data is often artificial, we argue that this case law of the Court unjustifiably applies different constitutional reasoning to these two types of data. This is particularly true because the Court itself recognises, in *Tele2 Sverige*, that 'establishing a profile of the individuals' – on the basis of metadata – 'is no less sensitive, having regard to the right to privacy, than the actual content of communications'.[30]

It is important to clarify that the Court in *Schrems* does not seem to find problematic every access to content to electronic communications, but only a generalised access to content[31] by public authorities.[32] In practice, that would be access to content of all e-mail or mobile phone communications without a reasonable suspicion that the users have been involved in a crime. The Court's case law seems to imply that if the access is individualised, this could not lead to an impairment of essence of the fundamental right to privacy, but would be assessed under the traditional proportionality analysis. In practice that means for example that access to an e-mail account in the framework of a criminal investigation would interfere with the right to privacy (Article 7) of the e-mail account holder, but that such an interference could be justified by the purposes of a criminal investigation, provided it is proportionate with that purpose.

---

[27] *Schrems*, para 95.
[28] Schrems, para 94.
[29] *Tele2 Sverige*, para 107.
[30] *Tele2 Sverige*, para. 99. In this regard, the CJEU follows the Opinion of the Advocate General Saugmandsgaard Øe and also expressly cites paragraphs 253, 254 and 257 to 259 of his opinion.
[31] *Schrems*, para 94.
[32] *Schrems*, para 93.

Moreover, the Court's case law deals with generalised government access for the purpose of criminal investigations. The circumstance that, in *Schrems*, the access by public authorities was at stake does, however, not mean that private parties (such as telecommunications operators) are authorised to access the content of electronic communications in a generalised way. Even though there is no indication that the same strict assessment would be applied for generalised access by the private sector, such access would always need to be justified by overriding reasons and proportionate with the aim pursued, which would, in practice, amount to balancing of rights and interest of both parties involved.

We could imagine the possibility of restricted access for purposes that do neither aim at interfering with individuals' privacy rights, nor have the effect of such interference. An example is access with the rationale of delivering better services, such as machine learning applications or personal assistance (like automated translations or voice to text applications). Of course, it should be ensured that individuals' rights are effectively protected, including effective remedies.

Finally, the case law of the Court of Justice specified the particularly sensitive nature of content data and metadata. However, it is important to note that content data and metadata are not included in Article 9 of the GDPR on specific categories of data which enjoy a higher protection and cannot be processed on the basis of the legitimate interest of the controller.

Application of the Charter right to privacy to legal persons

There is a constitutional broader debate on the question whether legal persons, in particular companies, should be able to invoke certain fundamental rights from the Charter. While a comprehensive analysis of the constitutional theory in this regard exceeds the scope of this legal note, it is nevertheless important to stress that legal persons are not entirely without fundamental rights protection under EU law.

However, this protection is limited only to particular fundamental rights. Already in one of the first fundamental rights cases to reach the Court of Justice, *Nold*, the applicant was a German company ('limited partnership governed by German law'), invoking its fundamental right to property and freedom to pursue economic activity.[33] The Court, in its seminal judgment, not only expressly accepted these fundamental rights as part of the (then) European Community legal order,[34] but implicitly also recognised that Nold, as a legal person, can rely on these rights. Further, in a more recent case, *DEB*, the Court of Justice recognised that legal persons can invoke the principle of effective judicial protection, enshrined in Article 47 of the Charter.[35]

[33] Case 4/73, *Nold v Commission*, ECLI:EU:C:1974:51.
[34] *Nold*, para 14. To be precise, the ruling applied to the legal order of the European Community, the predecessor of the EU.
[35] Case C-279/09, *DEB*, ECLI:EU:C:2010:811, para 63.

The European Court of Human Rights (ECtHR) similarly recognised the possibility to apply certain fundamental rights to companies, such as freedom of expression under Article 10 ECHR[36] and the respect for home and correspondence protected under Article 8 ECHR.[37] For example, in the *Niemietz v Germany* case, the ECtHR pointed out that an interpretation of the notions 'private life' and 'home' from Article 8 ECHR 'as including certain professional or business activities or premises' is in accordance 'with the essential object and purpose' of this provision.[38] In *Société Colas Est v France*, the ECtHR found a violation of Article 8 ECHR in a case of raid of companies by inspectors.[39] Another interesting case is *Vinci Construction and GTM Génie Civil et Services v France*, where the ECtHR found a violation of Article 8 ECHR due to dawn raids exercised in the framework of enforcement of EU competition law, due to the circumstance that a large number of documents, including confidential ones, was raided without the company it having the possibility to have an insight into this documentation during or after the raid.[40]

As correctly invoked by the European Commission in the Explanatory Memorandum to the proposal for the ePR,[41] such interpretation of Article 8 ECHR is valid also for its equivalent in the Charter (Article 7), given that Article 52(3) of the Charter requires that Charter rights should provide the same or more extensive protection than the ones from the ECHR.

It should be noted, however, that the abovementioned case law of the ECtHR refers to the part of Article 8 ECHR relating to the respect of 'home and correspondence' and not to the 'right to respect for private and family life'. Whereas the former can indeed be extended to encompass the rights of legal persons, the latter is inherent to the protection of individuals, not least because of the link of individuals' privacy with human dignity.[42] Article 7 of the Charter makes the same distinction in its text and refers to the protection of 'home and communications' separately from the protection of 'private and family life'. Even from a practical perspective, it is difficult to imagine how a company could invoke the right to privacy going beyond the protection of privacy of its premises and confidentiality of its communications.

For comparable reasons, the GDPR, which gives expression to the fundamental right to data protection (Article 8 of the Charter) specifically provides that the Regulation cannot be invoked by legal persons. Recital 14 of the GDPR provides that "[t]his Regulation does not

[36] Case *Sunday Times v United Kingdom*, App No 6538/74,, as cited by Peter Oliver, Companies and Their Fundamental Rights: A Comparative Perspective, 64 International and Comparative Law Quarterly, 677.
[37] See Oliver, op. cit., 677-678, and case law cited therein: *Niemietz v Germany*, App No 13710/88; *Société Colas Est v France*, App No 37971/97.
[38] *Niemietz v Germany,* para 31.
[39] *Société Colas Est v France*, para 50. For an analysis of the so called '*Colas Est* standard', see Marius Emberland, The Human Rights of Companies. Exploring the Structure of ECHR Protection (Oxford University Press 2006) 172 et seq.
[40] Case *Vinci Construction and GTM Génie Civil et Services v France*, App No 63629/10 and 60567/10, paras 74-81.
[41] Point 2.1.
[42] For the link between privacy and human dignity see Catherine Dupré, 'Commentary of Article 1 – Human Dignity', in Steve Peers et al. (eds), *The EU Charter of Fundamental Rights. A Commentary* (Hart 2014) 7, who stresses that 'dignity has often been associated with privacy'.

cover the processing of personal data which concerns 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 ground for distinction in applicability between Article 7 ('home and communications' part) and Article 8 of the Charter is therefore purposeful in nature: as legal persons do not have personal characteristics, they also do not have the right to personal data protection.

To conclude, legal persons are entitled to invoke the confidentiality of communications, an element of Article 7 of the Charter. However, this protection can be safeguarded also on the basis of other EU instruments, such as the Directive on the Protection of Trade Secrets,[43] outside of the scope of Article 7 of the Charter. They are not entitled to invoke Article 8 of the Charter.

- **In so far as ePR gives expression to the right to privacy (Article 7 of the Charter), potential limitations of this right to privacy in the ePR should respect Article 52.1 of the Charter.**

- **Neither Article 7 nor Article 52.1 of the Charter enumerate the grounds for limitation of fundamental rights. They do not prescribe that the right to privacy can be limited only on the basis of particular justificatory grounds, such as consent of the user. The legislator may limit this fundamental right for other reasons such as the legitimate interest of the provider of electronic communications, or justified interests of society..**

- **Effective remedies for individuals must always be provided and safeguarded.**

- **The Court of Justice specified the particularly sensitive nature of content data and metadata, although these data are not included in Article 9 of the GDPR on specific categories of personal data which cannot be processed on the basis of the legitimate interest of the controller.**

- **Legal persons are entitled to invoke the confidentiality of communications, an element of Article 7 of the Charter. The protection can be safeguarded also on the basis of other EU instruments, such as the Directive on the Protection of Trade Secrets (outside of the scope of Article 7 of the Charter). Legal persons are not entitled to invoke Article 8 of the Charter.**

[43] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157/1.

SECTION 3. SAFEGUARDS FOR PROTECTION OF FUNDAMENTAL RIGHTS IN THE GDPR

In a previous study for CIPL "EPR vis-à-vis GDPR[44], it was demonstrated that there are only very limited cases where the processing of electronic communications data would not constitute processing of personal data covered by the GDPR.

The ePR will apply to data that are not subject to the safeguards in the GDPR only in very exceptional circumstances, such as pure machine-to-machine communications, where there is no involvement of natural persons, and hence, where the communications data does not relate to an identified or identifiable individual, will the ePR apply to data that are not subject to the safeguards set forth by the GDPR. As mentioned above, it could be argued that these situations actually fall outside the scope of the protection of the fundamental right to privacy (article 7 of the Charter), as this right is ultimately aimed at protecting human dignity.

As, in practice, almost any processing of electronic communications data, including communications content and metadata, will be subject to the GDPR. Hence, it should be assessed whether the safeguards provided for by the GDPR are sufficient to ensure that the limitation to the confidentiality of communications resulting from the processing of electronic communications data meet the test of Article 52.1 of the Charter (as described above).

One of the key questions for this test is whether the fact that the GDPR applies to any processing of data relating to electronic communications involving natural persons is sufficient to ensure that the right to privacy set forth in Article 7 of the Charter is respected.

The GDPR set forth a robust set of rules, safeguards and limitations that must be respected by organizations when processing personal data and provides for effective remedies to enforce these. Due to the broad scope of the GDPR, these rules, safeguards and limitations will apply to almost any processing of electronic communications data by anyone, including providers of electronic communications networks and services.

Article 5 of the GDPR sets forth the general principles that must be respected when processing personal data – i.e., (i) lawfulness, fairness and transparency, (ii) purpose limitation, (iii) data minimization, (iv) accuracy, (v) storage limitation, (vi) integrity and confidentiality, and (vii) accountability. These general overarching principles are further fleshed out in more detailed obligations throughout the GDPR. Finally, GDPR includes a risk based approach (discussed below). This requires organisations to calibrate their compliance and safeguard measures based on risk and harms to individuals stemming from a particular data processing.

[44] EPR vis-à-vis GDPR: A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation, prof. dr. G-J. Zwenne LLM, Quinten Kroes LLM, and Joost van Eymeren LLM, July 19, 2018 (available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-brinkhof_epr_study.pdf).

One of the key aims of the ePR is ensuring the confidentiality of communications content and metadata. As mentioned above, confidentiality is also one of the core principles of the GDPR and the GDPR imposes various obligations requiring organizations to ensure the confidentiality of the personal data they process. In particular, Article 32 of the GDPR requires organizations to implement technical and organizational measures to ensure an appropriate level of security for the personal data they process, including measures to ensure the ongoing confidentiality of processing systems and services. This Article reflects the risk-based approach chosen by the EU legislator in the GDPR. Organizations are required to assess the risks that are presented by their data processing activities, including the risks presented by unauthorized disclosure of or access to personal data that are transmitted, stored or otherwise processed, and implement measures that ensure a level of security that is appropriate to those risks.

Although electronic communications data are not explicitly recognized as a special category of personal data requiring an additional level of protection under Article 9 of the GDPR, the sensitive nature of this type of data has been recognized by the CJEU[45] and by EU data protection authorities.[46]

This implies that, under the GDPR, organizations that process electronic communications data are required to put in place robust security (including confidentiality) measures, as the sensitive nature of this type of data presents high risks.

This risk-based approach, triggering a high level of protection for electronic communications data, is also at the core of Article 24.1 of the GDPR, which requires data controllers always to take "*into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons...*". This general accountability obligation is further fleshed out in a number of specific measures that organizations should or must take. These measures include:

- Adopting data protection policies, including for example policies around handling requests from data subjects who exercise their data protection rights;
- Putting in place measures to ensure that data protection is taken into account during the entire data processing lifecycle (i.e., data protection by design and by default);
- Ensuring that written agreements are in place with third parties processing personal data on the organization's behalf;
- Maintaining internal records of the organization's data processing activities;

[45] Cases *Schrems* and *Digital Rights Ireland*, discussed above.
[46] See, for example, Guidelines of the Article 29 Working Party on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Communications data are also included in the DPIA lists of a number of national data protection authorities, https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

- Carrying out data protection impact assessments and, in certain cases, consulting with the relevant supervisory authority prior to commencing a data processing activity;

- Documenting data security measures;

- Notifying personal data breaches to supervisory authorities and the affected data subjects, as well as keeping internal documentation on such personal data breaches;

- Appointing a data protection officer; and

- Identifying data transfers to non-adequate countries outside the EU and putting in place appropriate data transfer mechanisms.

Whether or not it is appropriate or required to put in place the accountability measures listed above and how robust these measures should be, to a certain extent, depends on the risks the organization's processing activities present to the rights and freedoms of individuals. Taking into account the sensitive nature of electronic communications data, whose confidentiality should be protected in light of the right to privacy under Article 7 of the Charter, organizations that process this type of data will, in light of the risk-based approach under the GDPR, typically be required to put in place robust accountability measures. Certainly, processing of electronic communications data is likely to require organisations to conduct a specific data protection impact assessment. This is also emphasised on several occasions by data protection authorities. Authorities have specifically included processing of electronic communication data (metadata and content) in the lists of high risk processing requiring a Data Protection Impact Assessment (DPIA) under the GDPR. This was recently confirmed by the European Data Protection Board.[47]

The accountability requirements also have a link with the legal basis on which the organization relies to legitimize its data processing activities. Organizations that rely on their legitimate interests or the legitimate interests pursued by a third party (Article 6, §1 (f) of the GDPR) as a legal basis to process individuals' personal data are required to carry out and document a balancing test to ensure that the interests or fundamental rights and freedoms of the individuals whose personal data they process are not overriding. This balancing test is not just a paper based, tick-the-box exercise. It actually requires an in depth consideration from companies of a number of factors, to ensure that the interests and fundamental rights of the individuals whose personal data they process are duly taken into account. This includes the factors identified by the Article 29 Working Party in its Opinion on the notion of legitimate interests of a data controller under the Data Protection Directive, which are still relevant under the GDPR:

- The nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned;

[47] https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

- The impact on the concerned individuals and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed; and

- Additional safeguards which could limit undue impact on the concerned individuals, such as data minimisation, privacy-enhancing technologies, increased transparency, general and unconditional right to opt-out, and data portability.[48]

Furthermore, organizations are required to provide individuals with information from the balancing test or, at least, make clear in their privacy notice that the concerned individuals can obtain information on the balancing test upon request. This enables the concerned individuals to assess whether the balancing test has been carried out fairly or whether they could file a complaint with a supervisory authority.[49]

Taking into account these increased accountability and transparency obligations, it could be asserted that, in practice, individuals privacy rights may ultimately benefit from a strong protection if an organization relies on legitimate interests as a legal basis for processing his or her personal data, including electronic communications data. The traditional concept of the communication secrecy, as reflected in the ePR, still heavily focuses on consent. Although this gives individuals, at least in theory, the highest level control over the processing of their data, it may not always result in a better protection of their right to privacy in practice.

If an organization obtains the concerned individuals' consent, there is a certain presumption that the rights and interests of the concerned individuals and the organization are balanced. In contrast, where a company relies on the legitimate interest ground, it must implement additional measures to ensure that its processing activities pass the balancing test, in particular when processing data of a sensitive nature such as electronic communications data. In practice, these additional measures may include limiting the data that are processed to a strict minimum, implementing short data retention periods, anonymizing data to the extent possible, using aggregated data, carrying out in depth Data Protection Impact Assessments, implementing measures and/or procedures to facilitate individuals in exercising their data protection rights, such as the right to opt-out and data portability.

As mentioned by the Article 29 Working Party, the legitimate interest ground "*presents complementary safeguards - which require appropriate measures - compared to the other pre-determined grounds*"[50], such as consent. A real life example of what appropriate measures may include is the monitoring of ICT use of employees, included in the Annex.

[48] See Article 29 Working Party's Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.
[49] See Article 29 Working Party Guidelines on transparency under Regulation 2016/679.
[50] See Article 29 Working Party's Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

- **The GDPR sets forth a robust set of rules, safeguards and limitations that must be respected by organizations when processing personal data and provides for effective remedies for individuals to enforce these. The GDPR will apply to almost any processing of electronic communications data.**

- **The GDPR requires organizations that process electronic communications data to put in place robust security and confidentiality measures. The accountability and risk-based approach are the core of the GDPR (Article 24). This will result in organisations having to implement heightened protection, safeguarding measures and DPIAs, to reflect that processing of this type of data may result in high risks to individuals rights and freedoms.**

- **Individuals' privacy rights actually may benefit from a strong protection if an organization relies on legitimate interests as a legal basis for processing electronic communications data, due to the increased accountability measures organisations need to take.**

ANNEX

A real life example of the type of additional safeguards organisations must put in place, is the monitoring of ICT use of employees (e.g., email, phone, internet browsing, instant messaging, VOIP), which should respect the requirements of the ruling of *Bărbulescu v. Romania*.[51] Examples of necessary safeguards that companies must consider under the GDPR are:

(i) Measures to prevent/limit personal use of company devices and the professional email account (e.g., implementing a clear acceptable use policy),

(ii) data-oriented limitations that prevent monitoring of personal files or communications (e.g., requiring employees to store personal emails and files in a dedicated folder clearly marked as "personal", or to mark personal appointments in their calendar as "personal", limit monitoring in the context of BYOD by providing the option to sandbox or ring-fence data on personal devices or implementing other measures to distinguish personal and professional use on the employee's device),

(iii) impose clear rules for systems/individuals performing the monitoring (e.g., use relevant key word searches and similar techniques to limit monitoring to relevant information, immediate erasure of false positives, etc.);

(iv) perform monitoring in different stages (i.e., first at company level without identification of specific employees and only individualize monitoring results if serious issues or infringements are detected, possibly after issuing a warning to employees with respect to the findings of the monitoring at company level); limit monitoring in time (i.e., occasional instead of permanent monitoring, limit monitoring outside working hours, etc.);

(v) providing clear information with respect to the company's monitoring practices, both to employees individually (e.g., through a clear employee monitoring notice and policy, specific just-in-time warnings, etc.) and, if required or appropriate, collectively (i.e., to the works council or other employee representative bodies);

(vi) (continuously) assess whether there exist less privacy-invasive means to achieve the purpose of the monitoring (e.g., security of the company network);

(vii) provide alternative unmonitored communications means (e.g., standalone devices that employees can use for limited private usage);

(viii) take preventive measures to avoid misuse or malicious behaviour (e.g., website blocking);

[51] European Court of Human Rights, 5 September 2017, App. No. 61496/08.

(ix) implement organizational safeguards (e.g., appoint a trusted person to perform the monitoring, limit the number of persons performing the monitoring and having access to the monitoring results on a strict need-to-know basis and ensure that these persons are bound by strict confidentiality obligations and that they are aware of the purposes and instructions for the use of the data, as well as applicable data protection/privacy rules and procedures);

(x) implement measures to ensure that the data processed in the context of the monitoring receive the same level of protection as they did before the monitoring (e.g., specific protection of data about members of employee representative bodies); and

(xi) document decision to monitor and monitoring protocol (including the facts, suspicions, allegations and concerns that triggered the decision to monitor; the measures implemented to ensure that the concerned employees' rights and the company's interests are properly balanced; and confirmation that less intrusive measures were considered and the reasons why these were not deemed sufficient), as well as the monitoring process (e.g., who performed the monitoring, on whose behalf, when, why and who had access to the monitoring results).