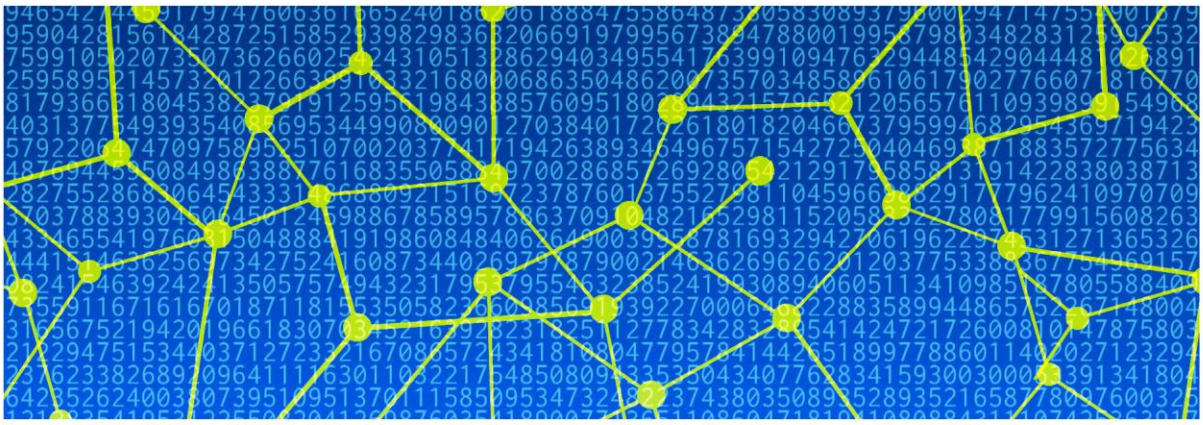

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 4/2017

on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content

EDPS

14 March 2017

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41.2 of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies", and "…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with Assistant Supervisor with the specific remit of being more constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking -in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. The EDPS considers that compliance with data protection requirements will be key to the success of EU consumer protection law in the Digital Single Market.

Executive Summary

The EDPS acknowledges the importance of the data-driven economy for the growth in the EU and its prominence in the digital environment as set out in the Digital Single Market strategy. We have argued consistently for the synergies and complementarity between consumer and data protection law. We therefore support the aim of the Commission's proposal of December 2015 Directive on certain aspects concerning contracts for the supply of digital content to enhance the protection of consumers who are required to disclose data as a condition for the supply of 'digital goods'.

However, one aspect of the Proposal is problematic, since it will be applicable to situations where a price is paid for the digital content, but also where digital content is supplied in exchange for a counter-performance other than money in the form of personal data or any other data. The EDPS warns against any new provision introducing the idea that people can pay with their data the same way as they do with money. Fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity.

The recently adopted data protection framework (the "GDPR") is not yet fully applicable and the proposal for new e-Privacy legislation is currently under discussion. The EU should avoid therefore any new proposals that upset the careful balance negotiated by the EU legislator on data protection rules. Overlapping initiatives could inadvertently put at risk the coherence of the Digital Single Market, resulting in regulatory fragmentation and legal uncertainty. The EDPS recommends that the EU apply the GDPR as the means for regulating use of use of personal data in the digital economy.

The notion of "data as counter-performance" - left undefined in the proposal - could cause confusion as to the precise function of the data in a given transaction. The lack of clear information from the suppliers in this regard may add further difficulties. We therefore suggest considering, as a way of resolving this problem, using the definition of services under the TFEU or the provision used by the GDPR to define its territorial scope.

This Opinion examines the proposal's several potential interactions with the GDPR.

First, the broad definition of "personal data" under data protection legislation may well have the effect that all data subject to the Proposed Directive be considered as "personal data" under the GDPR.

Second, the strict conditions under which a processing can take place are already set down in the GDPR and do not require amendment or addition under the proposed directive. While the proposal seems to consider as legitimate the use of data as a counter-performance, the GDPR provides, for example, a new set of conditions to assess the validity of consent and to determine whether it can be considered as freely-given in the context of digital transactions.

Finally, the proposed rights given to the consumers to obtain their data from the supplier at the termination of the contract and the obligation for the supplier to refrain from using data potentially overlap with the rights of access and to portability and with obligation of the supplier to refrain from using the data and data controller obligations under the GDPR. This might unintentionally lead to confusion regarding the regime applicable.

TABLE OF CONTENTS

1. INTRODUCTION AND BACKGROUND 5

1.1. THE CONSULTATION OF THE EDPS BY THE COUNCIL 5

1.2. THE PROPOSAL 6

2. THE USE OF PERSONAL DATA AS "COUNTER- PERFORMANCE" 6

2.1. PERSONAL DATA AS COUNTER-PERFORMANCE AND THE FUNDAMENTAL RIGHT TO DATA PROTECTION 7

2.2. ARTICLES 8 OF THE CHARTER OF FUNDAMENTAL RIGHTS AND ARTICLE 16 TFEU 8

2.3. THE NOTION OF DATA AS "COUNTER-PERFORMANCE" 9

2.4. POSSIBLE ALTERNATIVES 10

3. FURTHER ANALYSIS OF THE PROPOSAL 11

3.1. THE SCOPE OF THE PROPOSAL 11

a) The notion of personal data 11

b) The personal data triggering the application of the Directive 12

c) The data excluded from the application of the Directive 13

3.2. THE POSSIBLE LEGAL BASIS FOR PROCESSING 13

a) Considerations regarding the grounds for processing 14

b) The different grounds for processing of data in the context of the Proposal 14

3.3. THE WITHDRAWAL OF CONSENT 18

3.4. THE RIGHTS TO ACCESS ONE'S DATA AND THE RIGHT TO PORTABILITY 18

a) The rights to object, erasure, object and the right to data portability 18

b) Interaction with the Proposal 19

NOTES 22

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty of the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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[1], and to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[2],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[3], and in particular Articles 28(2), 41(2) and 46(d) thereof,

1. INTRODUCTION AND BACKGROUND

1.1. The consultation of the EDPS by the Council

1. On 9 December 2015, the European Commission presented two legislative proposals for new contractual rules for online sales. The proposed digital contract rules include two draft pieces of legislation:

- a Proposal for a Directive on certain aspects concerning contracts for the supply of digital content[4];
- a Proposal for a Directive on certain aspects concerning contracts for the online sales of (tangible) goods[5].

2. The two proposals are to be seen as a package with common objectives, notably to remove the main obstacles to cross-border e-commerce in the EU[6]. As regards more specifically the Proposal for a Directive on contracts for supply of digital content to consumers (hereinafter "the Proposal"), its intention is to have a single set of rules covering contracts for the sale and renting of digital content as well as contracts for digital services[7]. At the time of the adoption of the Proposal, the EDPS was not consulted by the Commission.

3. On 21 November 2016, the LIBE Committee issued an Opinion on the Proposal[8]. The European Parliament Internal Market and Consumer Protection Committee (IMCO) and the Legal Affairs Committee (JURI) issued a draft joint report on the Proposal on 7 November 2016[9].

4. The Council is currently discussing the Proposal within the Working party on Civil Law Matters (Contract law). In this context, on 10 January 2017, the Council decided to consult the EDPS on the Proposal. The EDPS welcomes the initiative of the Council to consult the EDPS on this important legislative which raises many questions in relation to the Union law on the

protection of personal data. The present Opinion is the EDPS' response to the request of the Council.

1.2. The Proposal

5. Currently, the supply of digital content at EU level is partly regulated by the Consumer Rights Directive[10], Unfair Terms Directive[11] and e-Commerce Directive[12]. The Consumer Sales Directive is not applicable, as the definition of 'consumer goods' in that Directive extends only to 'tangible moving items'.

6. Several Member States have already adopted specific rules for digital content, creating differences in scope and content between the national rules governing these contracts[13]. The Proposal therefore intends to provide for a harmonised protection of the consumers so far as digital content is concerned. In this context, the Proposal envisages a maximum level of harmonisation.

7. As to the scope of the Proposal, it would cover not only digital goods (such as films or music, computer programs, mobile applications, ebooks) but also digital services (such as social media platforms and cloud computing services). For a digital contract to fall within the scope of the proposed directive, it must either provide for a price to be paid by the consumer, or the consumer must "actively provide personal data or other data as counter-performance"[14].

8. The Proposal introduces a "hierarchy of remedies" in case of lack of conformity of the digital content or service provided by the seller, and provides for the consumer's right to retrieve the data at the termination of the contract in a "commonly used data format"[15]. The Proposal also imposes the obligation for suppliers to refrain from the use of the data provided as counter-performance after the termination of the contract[16].

9. The Proposal refers to the concept of personal data in three situations:
- the use of data (including personal data) as a "counter-performance other than money"[17];
- a reference to data which is "strictly necessary for the performance of the contract"[18];
- a reference to "other data produced or generated through the consumer's use of the digital content"[19].

10. The reference to the concept of personal data creates a potential interaction between the Proposal and the data protection rules, as laid down, among others, in the Data Protection Directive 95/46/EC[20] and the GDPR[21]. Furthermore, as stated in the Proposal, the Directive is intended to be without prejudice to the protection of individuals with regard to the processing of personal data[22]. This Opinion will therefore address the interplay between the Proposal and the current and future EU data protection framework[23].

2. THE USE OF PERSONAL DATA AS "COUNTER-PERFORMANCE"

11. The proposed Directive would apply to "any contract where the supplier supplies digital content to the consumer or undertakes to do so" in exchange of a price but also when "the

consumer actively provides counter-performance other than money in the form of personal data or any other data".

12. The scope of the Directive is so defined in order to ensure that ostensibly "free" contracts can also benefit from certain protections of the proposed Directive. Services generally considered as "free" are generally based on an economic model where personal data are collected by the providers in order to create value from the data processed.

13. The EDPS recognises the importance of the digital economy in the Union and the value of the data in the digital environment[24]. Therefore, the EDPS welcomes the initiatives of the Commission with the regard to the use of (personal and non-personal) data and to foster the data-driven economy. The new data protection framework, which will be applicable as of 25 May 2018, has been redesigned in order to address the opportunities and the challenges of the use of data in such a context. In this context, the EDPS' mission is to help the legislator to approach the regulation of this market by taking into consideration the implications for the individuals regarding their fundamental right to the protection of their personal data.

14. The EDPS welcomes the intention of the legislator to make sure that the so-called "free services" are subject to same protection for the consumers when they do not pay a price for a service or content. However, personal data cannot be compared to a price, or money. Personal information is related to a fundamental right and cannot be considered as a commodity. Elaborating on this assumption, the following sections present the reasons why the EDPS recommends avoiding the use of the notion of data as counter-performance in the Proposal, and presents alternative options to replace the use of such a notion.

2.1. Personal data as counter-performance and the fundamental right to data protection

15. The business models of "free services" have already been addressed by the EDPS in previous Opinions[25]. For many digital services, companies foster the perception that they are provided for free, while in fact individuals are required to surrender valuable information. In effect, providers require the disclosure of personal information, often without the knowledge of the individual, as a condition for the supply of the service. The extent to which companies should be able to leverage and to monetise the personal datasets acquired has been subject of some debate.

16. As already stated in his Opinion 08/2016 that "*in the EU, personal information cannot be conceived as a mere economic asset. According to the case law of the European Court of Human Rights, the processing of personal data requires protection to ensure a person's enjoyment of the right to respect for private life and freedom of expression and association. Furthermore, Article 8 of the EU Charter and Article 16 of the Treaty on the Functioning of the European Union (TFEU) have specifically enshrined the right to the protection of personal data. In consequence, the 2016 General Data Protection Regulation contains specific safeguards that could help remedy market imbalances in the digital sector*"[26].

17. There might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation. One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction[27].

18. In seeking to enhance the protection of the consumer of online goods, **the Proposal raises a number of issues given the fundamental rights nature of these data and the specific protection granted to these data under the EU data protection framework (see Section 3 below).**

2.2. Articles 8 of the Charter of Fundamental Rights and Article 16 TFEU

19. As mentioned above, the right to protection of personal data is enshrined in Article 8 of the Charter of Fundamental Right of the EU ("the Charter") and Article 16 of the TFEU. According to Article 8 (2) of the Charter, data must be *"processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified"*.

20. The principles of **Article 8 of the Charter** are further specified in secondary EU legislation: the Directive 95/46, to be replaced by the GDPR, and the e-Privacy Directive (to be replaced by the e-Privacy Regulation). These texts lay down the requirements for a consent to be valid, provide for the key principles such as the "purpose limitation principle"[28], and establish data subjects' rights, such as the right of access. The Proposal, by introducing the explicit possibility to use personal data as counter-performance, and by creating an ad hoc regime for the access of the consumers to their personal data, **interferes with Article 8 (2) of the Charter and the data protection principles as provided by the Directive 95/46, the GDPR and the "e-Privacy Directive"[29].**

21. The Proposal, however, is not the proper instrument to regulate the use of personal data: the GDPR was adopted for this purpose, and aimed at stating the new rules regarding the use of personal data, on the basis of Article 16 TFUE which is specifically dedicated to data protection. Therefore, **the Proposal, based on Article 114 TFEU, should avoid including provisions which may have an impact the data protection framework.**

22. In this context, the EDPS stresses that while Directive 95/46 was already adopted on the basis of Article 114 TFEU (ex-95 TEC), the GDPR also refers to the internal market, aiming to prevent obstacles to the free flow of data within the Union[30]. Therefore, internal market considerations, including the digital environment, were already taken into account when discussing the GDPR[31].

23. One of the aims of the GDPR was to provide trust that will allow the digital economy to grow within the internal market[32]. The GDPR already considered the different business models using personal data, such as the "free" services which are subject to the Proposal. The GDPR also intends to enhance legal certainty for operators and individuals[33]. For these reasons, any change to the results achieved by the GDPR should be avoided, in order to preserve the political choices concerning the use of the personal data in the digital market. While the GDPR will only be applied as of 25 May 2018, any provision that would impact directly or indirectly the use of personal data should be avoided. Moreover, such initiatives may create legal uncertainty

and can undermine the coherence of the legal framework applicable to the digital economy and could lead to regulatory fragmentation in the Digital Single Market. Therefore, although the EDPS notes that the intention of the EU legislator is not to restrict or derogate from the data principles[34], **by no means should the Proposal change the balance found by the GDPR regarding the circumstances under which the processing of personal data may take place in the digital market.**

2.3. The notion of data as "counter-performance"

24. The EDPS has serious doubts about the use of the notion of counter-performance by the Proposal in the context of the relationships between the consumers and the suppliers. This section lists several reasons why the EDPS urges caution when considering that data can be used as a counter-performance.

25. **First**, the Proposal does not define what is understood as a counter-performance. It seems that the Proposal makes a link with the value of information about individuals, which would be comparable to money. However, several uses of personal data for other purposes than the strict performance of the contract can be observed: data can be used to improve the quality of the service, to provide personalised services to consumers, to improve security, to sell or licence consumer data. Adding to this confusion, the Proposal excludes certain categories of data from its scope, such as in situations where "the supplier does not use that data for commercial purpose"[35]. However, considering that the Proposal will apply in the context of a commercial transaction, one can presume that the use of data by the suppliers will always be for a commercial purpose. Considering the various business models and different uses of personal data in the context of a commercial transaction, the use of the term counter-performance is not appropriate to address the business models at stake and could appear to oversimplify in one single term a variety of business models and data usages.

26. **Second**, the link made by the Proposal between paying a price with money, and actively giving data as a counter-performance is misleading. While the consumer is aware of what he is giving when he pays with money, the same cannot be said about data. Standard contractual terms and privacy policies do not make it easy for the consumer to understand what is precisely made with the data collected about him/her. In this context, it has already been debated whether the organisations could be required to reveal more about their decision making in data processing operations[36], for example about their intention to create value with the data. It can be observed that privacy policies typically contain vague and elastic terms for the description of the use of the data collected, like "improving consumers' experience"[37]. Issues of transparency and fairness in terms and conditions of several online services have been raised through some national investigations into social media and other online services[38].

27. **Third**, it should be reminded that if personal data might be compared with money to some extent, they are obviously not identical. Giving his/her data does not deprive the individual from the possibility to give the same data again to another provider. Moreover, as said above, the individuals cannot evaluate the value that will be created with their data. The consequence for the providers is also different: when an obligation of restitution exists[39], such restitution is

easy when a price was paid, while is more difficult when data were exchanged. There is indeed little possibility to evaluate the value of personal data, and therefore to "reimburse" the individual on the basis of the value of these data, or even to give him/her a compensation for the value gained by the supplier in the transaction.

28. The above shows that it will be difficult, and sometimes impossible, to easily identify the cases where personal data are actively provided as counter-performance for the provision of a "free" digital services or contents, which is the element triggering the application of the Directive for "free" services. It will therefore also be difficult for the consumer, the regulators, the judges and even the providers to determine when this Directive will be applicable, leading to legal uncertainty. Although the proposal seeks to protect consumers, it rather legitimises a practice without taking into account the specific nature of personal data. In doing so, it may alter the balance struck in the GDPR (see above, Section 2.1). For these reasons, **the EDPS considers that the term "data as a counter-performance" should be avoided.**

2.4. Possible alternatives

29. The EDPS reaffirms that he welcomes the intention of the Commission to protect consumers even in cases where they did not pay a price for the digital content received. However, as explained, **one should avoid treating personal data as a commodity as any other, for reasons mentioned above.** If the intention of the legislator is to make sure that those offering "free" digital goods in exchange for personal data fall within the scope of the draft Proposal, other approaches might be explored so as to avoid any implications of data acting as counter-performance. In offering these suggestions, the EDPS is not in any way questioning the EU's approach to contract law, nor drawing any conclusions regarding their compatibility with consumer protection law.

30. Firstly, EU law recognises a broad definition of a "service"; indeed, according to Article 57 TFEU, "services shall be considered to be 'services' within the meaning of the Treaties where they are normally provided for remuneration"[40]. The CJEU also recognised that the remuneration does not always have to be paid by the consumer[41]. This approach has been adopted in the so-called "e-commerce Directive[42]" (which the Proposal explicitly intends to supplement[43]), but also in the recent recast Proposal of the European Electronic Communications Code ("EECC")[44]. **The use of this notion of "services" can therefore be suggested as an alternative so as to encompass services where a price is not paid,** so as to maintain the broad protection that the Commission intended to provide to the consumers.

31. The Proposal intends to exclude from its scope some situations, such as where the consumer is exposed to advertisements exclusively in order to gain access to digital content[45]. Should the legislator still want to exclude certain business models from the regime set by the Proposal (although the intention seems to be to offer a broad protection to the consumers), it should be possible to mention in the Proposal the list of services which would be excluded from the scope of the Proposal.

32. **A second option relates to** the provision defining the territorial scope of the GDPR. Article 3 (2) (a) of the GDPR provides indeed that the GDPR will apply to the processing of personal data of data subjects who are in the Union by a controller or processor not established

in the Union, where the processing activities are related to "*the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union*". The scope of the GDPR is thereby not made dependent on the existence of any payment of counter-performance of any kind, since the mere offering of goods and services is the element triggering the applicability of the GDPR.

33. **The use of the definition of services -as this was for example done in the e-commerce Directive- could therefore be an alternative to delineate the scope of the Proposal and encompass the services where a price is not paid but which are normally provided for remuneration. This still leaves the possibility for the legislator to exclude certain categories of digital content services from its scope.**

34. **As another alternative, the Proposal could also use similar terms to the GDPR (referring to the offering of goods and services irrespective of whether a payment is required) in order to define the scope of the Proposal, without making reference to data used as counter-performance.**

3. FURTHER ANALYSIS OF THE PROPOSAL

35. This section further analyses the Proposal from a data protection perspective, in order to explain the interaction between the Proposal and the data protection regime so as to ensure that the analysis will remain valid in the future, the present analysis will mainly focus on the GDPR, which will be applicable as of 25 May 2018.

3.1. The scope of the Proposal

a) The notion of personal data

36. Under Article 4(1) of the GDPR,
"personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

37. This definition is very similar to the one of Directive 95/46, and has been extensively commented in an Opinion of the Article 29 Working Party[46]. The notion of personal data is very broad and encompasses any information that can be linked to an individual. Article 3(1) of the Proposal states that the Directive shall apply to any contract where a price is paid or where the *"consumer actively provides counter-performance other than money, in the form a personal data or any other data".* **In the light of the broad definition of personal data, it is likely that almost all data provided by the consumer to the provider of the digital content will be considered as personal data[47].** The same conclusion is valid regarding the application of Article 13 of the Proposal regarding the end of the processing of data and the obligation of restitution of the data[48]. This issue is addressed below in Section 3.4.

b) The personal data triggering the application of the Directive

38. The Proposal refers to the need to avoid discrimination between business models where the consumer pays a price and business models where a counter-performance is given in another form, such as personal data[49]. **Nevertheless, the EDPS observes that the Proposal will not apply to certain situations even where personal data are used as counter-performance.** Indeed, for the proposed Directive to be applicable, the personal data must have been given *actively* to the provider[50]. The EDPS is of the opinion that this notion contradicts data protection law.

39. **First**, by doing so, **the Directive creates a distinction between personal data actively and non-actively provided which does not exist in data protection law.** The same protection applies to data collected knowingly by the organisation processing the data, or the data given actively by the individual. Individuals should even be particular more protected against any invisible processing of data, especially in the online environment where the consumers are not always aware of such processing of their data[51]. However, such data that will in any case be considered as personal data and are therefore not excluded from the data protection provided by EU legislation.

40. One can find a reference to the term "data provided" in Article 20 (1) of the GDPR, referring to the right to data portability. In this regard, the Article 29 Working party has issued a Document for consultation[52]. One can notice that the term provided is broadly interpreted by the Working Party, which defines the term "provided" as follows*:*

> *- **Data actively and knowingly provided by the data subject are included** in the scope of the right to data portability (for example, mailing address, user name, age, etc.);*
> *- **Observed data are "provided" by the data subject by virtue of the use of the service or the device**. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by fitness or health trackers.*

41. **Second, where personal data are not actively provided by the consumer, the supplier might nevertheless still use these data for the same purposes as the data actively provided by the consumer.** Therefore, since the Proposal is only triggered when the data are actively provided, the Directive will not be applicable to the other suppliers collecting the data directly from the consumers without affirmative action on their side. An adverse effect could even be that some suppliers will not ask for the data to be directly provided but rather collect and process the same data passively provided by the consumers, in order to avoid to be subject to the Directive.

42. **Third**, by excluding some categories of data other than those (actively) provided, the Proposal also contradicts existing rules in e-Privacy Directive[53] and the Proposal for an e-Privacy Regulation[54], according to which those data should be in several instances only be obtained through user's consent, *i.e.* actively.

43. **For these reasons, the EDPS recommends avoiding referring to data (actively) provided by the consumer since it contradicts the (existing and future) rules on data protection.**

c) The data excluded from the application of the Directive

44. With the intention to make sure that they would not be considered as data provided as counter-performance, Article 3(4) of the Proposal excludes the data that are "strictly necessary for the performance of the contract", or for meeting legal requirements, except if the data are processed in a way "incompatible with these purposes" or for "commercial purposes". This paragraph seems to paraphrase the definition of "data provided as counter-performance", by creating a presumption that data used for other purposes than for the performance of the contract, for ensuring that the digital content is in conformity with the contract, or for meeting legal requirements, are data used as counter-performance. This Article 3 (4) calls for some remarks.

45. **First**, according to Article 8 of the Charter and Article 5 of the GDPR[55], data shall be *"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".* This is the so called "**purpose limitation principle**" (see below Section 3.2.a). The conditions to consider a further use as compatible have been analysed by the Article 29 Working Party[56], and specified in the GDPR[57]. Any incompatible further use of data is therefore not allowed, except when this further use is *"based on the data subject's consent or on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard objectives referred to in Article 23 (1)"* of the GDPR. Article 3 (4) of the Proposal refers to a use of data which is in principle not allowed under data protection principles except under the conditions mentioned above. **For these reasons, the Proposal should clarify that it does not affect the rules on further processing and the conditions under which a further use is considered compatible under the GDPR.**

46. **Second**, as already stated above, the use of data for "commercial purposes" as stated in the Proposal, encompasses a broad range of uses in the context of a contract between a supplier and a consumer, since the processing of data are likely to be always considered as commercial. For this reason, the definition of "commercial purposes" is too vague and should be further specified in the Proposal.

47. **Third**, the EDPS reminds that the legitimate grounds allowing the processing of data are exhaustively listed in the Directive 95/46 and the GDPR. However, with a reading *a contrario* of Article 3 (4), it could be argued that data used by the supplier for other purposes than the ones identified in this provision would automatically be considered as legitimate. Therefore, **the Proposal should confirm that the extent to which personal data may be used shall be exclusively determined under the relevant provisions of the GDPR.** The following section briefly presents the legitimate grounds for the processing of data.

3.2. The possible legal basis for processing

48. The present section will briefly expose the different legal grounds on which a processing may take place under the data protection framework, before explaining how these different grounds can play a role in relation to the processing of personal data in the context of a contract, and more specifically of the provision of digital content.

a) Considerations regarding the grounds for processing

49. As the Directive 95/46, Article 6 of the GDPR provides an **exhaustive list of six legal grounds for the processing of personal data** (see below, Section 3.2.b)[58]. Therefore, a processing of personal data must always rely on one of these legal grounds for a processing to be allowed[59]. Considering the purpose limitation principle mentioned above[60], in case the processing pursues several purposes, each of them must rely on the appropriate legal ground.

50. According to Article 13 (1) (c) of the GDPR, the **purposes for which the data are processed must be provided to the individuals**. This obligation applies when the data are collected directly from the data subject, irrespectively of whether they were (actively or passively) provided or not. It is therefore mandatory under data protection law to identify clearly the reasons why data are collected and processed by the controller. More specifically, the GDPR provides for more information obligations in the following cases:

- According to Article and 7 (2) of the GDPR, when the legitimate ground for the processing is the consent and is given in the context of a written declaration which also concerns other matters, **the request for consent shall be presented in a manner which is clearly distinguishable from the other matters.**
- In addition, where the processing is **based on consent**, the controller shall also inform the data subjects of their right to withdraw their consent at any time[61].
- When the processing is **based on the legitimate interests**, the controller shall provide the data subjects with the interests pursued by the controller or by a third party[62].
- The controller shall also specify **whether the provision of data is a statutory or contractual requirement, or a requirement to enter the contract**, but will also specify **whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data[63]**. However, this does mean that the supplier can unilaterally determine which are the data necessary for the provision of the service/performance of the contract (see below, Section 3.2.b).

51. Considering the above, the mere statement from supplier that personal data are "used as a counter-performance" would therefore not meet the requirements of a specific, clear and granular information given to the individuals to understand the different uses of their data (*e.g.* direct marketing, profiling, sale of customers' profiles, etc.)".

b) The different grounds for processing of data in the context of the Proposal

52. According to Article 6 (1) (b) of the GDPR, data may be processed if the processing is "***necessary for the performance of a contract*** *to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"*. This may for example include the address provided by the user to the supplier of good for the delivery of the credit card details for the payment. As reminded by the Article 29 Working Party, *"this provisions has to be strictly interpreted and will not cover situations where the processing is not genuinely necessary for the performance of the contract, but rather unilaterally imposed on the data subject by the controller"*[64]. In other words, if the contract can be performed without the collection and the processing of the data, they should not be considered as *"necessary for the performance of the contract".* The fact that the purposes of the processing

is covered by contractual clauses drafted by the supplier will not automatically mean that the processing is necessary for the performance of the contract. In case the purpose for the processing is not compatible with the original purpose -the processing for the performance of the contract- another legal ground will be necessary[65].

53. Article 3 (4) of the Proposal excludes from its scope only the processing which is *"strictly necessary for the performance of the contract (...) and the supplier does not further process them in a way incompatible with this purpose".* This difference of terms in both texts might lead to confusion and is might be understood that the "data as counter-performance" can be used under Article 6 (1) (b) of the GDPR, while these data are not considered under data protection law as necessary for the conclusion of the contract.

54. A processing may also take place if it is **based on the consent** of the individual[66]. The different requirements for a consent to be valid have been largely developed by the Article 29 Working Party in an Opinion dedicated to the definition of consent[67]. Under Article 4 (11) of the GDPR, "consent" of the data subject *"means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".* The GDPR restricted the conditions regarding consent. Article 7 provides additional requirements for the consent to be valid. Among other things, Article 7(2) provides that "*when the data subject's consent is given in the context of a written declaration which also concerns other matters*", for example a contract, consent must be separate from the consent needed for the conclusion of the contract. This implies that the processing of personal data provided by the consumer to the supplier which are not necessary for the performance of the contract, or for another purpose than the strict performance of the contract, will need to be based on another ground, such as a freely given consent. In this case, this consent must be separate from the consent given to the contract (or terms and conditions) and required for the conclusion of the contract.

55. Another condition for the consent to be considered valid is that it must be **freely given**. This question of a free consent is addressed by Article 4 (11), 7 and Recitals 32, 42 and 43 of the GDPR. According to Article 7 (1), the burden of proof that the consent is (freely) given is on the controller. In this regard, Article 7 (4) provides that "*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".* Recital 43 further specifies this idea and provides that "*Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance".* Therefore, the GDPR creates a presumption that the consent is not freely given when it is a conditional to receive the provision of a service "despite such consent not being necessary for such performance"[68]. Moreover, Article 8 of the GDPR introduces specific rules regarding the validity of the consent given by minors in relation to information society services, imposing the consent is given or authorised by the holder of parental responsibility over the child.

56. In a digital environment, according to Article 5 (3) and Article 9 of the e-Privacy Directive[69], and considering the prevailing business models and the rise of the value of personal data as an asset, the legal basis for the processing of data in the data-driven economy shall be, in most cases, the free consent of the individuals. In this context, the public consultation on the e-Privacy Directive revealed that *"almost two thirds of respondents (64%) say it is unacceptable to have their online activities monitored in exchange for unrestricted access to a certain website, while four in ten (40%) avoid certain websites because they are worried their online activities would be monitored"*[70]. The Proposal for an e-Privacy Regulation provides that the conditions of the GDPR shall apply regarding the validity of consent under the e-Privacy rules[71]. Therefore, **all conditions around consent introduced by the GDPR shall apply to the processing of data in the context of the provision of digital content under the Proposal.**

57. A joint reading of Article 7 and Recitals 32, 42 and 43 of the GDPR places the burden of proof that consent has been freely given on the controller. When the processing of data of a supplier is based on consent, it will therefore be up to him to demonstrate that the conditions concerning the validity of consent have been met. Several elements can be taken into account to assess the free character of the consent given by the consumer.

58. One of these elements will be the **transparency** of the processing, which mainly depends on the information given to the consumer regarding the processing. According to the GDPR, "*For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended"*[72]. The Article 29 Working Party has already encouraged granularity while obtaining the consent of the user, *"i.e. by obtaining separate consent from the user for the transmission of his data to the developer for these various purposes"*[73]. However, it is very rare that the supplier explicitly states that the data will be used as a counter-performance, or even to which specific purposes they will be processed[74]. Instead, as already mentioned[75], the controllers have to identify every specific use of the data (such as marketing, profiling, communication to third parties, provision of added value service, etc..).

59. The **imbalance** between the controller and the data subjects might also be taken into consideration[76]. Depending of the positions of the parties, the information asymmetry, or the possibility to choose another service, the data subject might be in a position where he/she does not have a choice but to consent to the processing to access a service, a product, or a digital consent.

60. The existence of a free choice for the individuals could also be assessed by the existence of **alternatives.** In the context of "free services", the Working Party already acknowledged that *"as long as such alternatives services are not available, it is more difficult to argue that a valid (freely given) consent has been granted"*[77]. What is considered as an alternative in this context might depend, among others, on the position of the supplier on the market or on the genuine existence of equivalent alternatives for the data subject[78].

61. In his preliminary Opinion on the review of the e-Privacy Directive, the EDPS already recommended that *"the new provisions on e-Privacy should provide that no one shall be denied*

*access to any information society services (whether these services are remunerated or not) on grounds that he or she has not given his or her consent under Article 5(3)"*and suggested several situations where consent should not be considered as free[79].

62. For these reasons, the admissible cases where consent should be considered as valid under the GDPR and the e-Privacy Directive/Regulation are to be assessed on a case by case basis[80], considering the rebuttable presumption created by the GDPR[81] and the strict conditions for the consent to be valid. A joint reading of the Proposal and the GDPR may lead to think that this presumption has been overturned by the Proposal, which would legitimize the processing of data based on consent in the context of a contract even when they are not necessary for the performance of the contract.

63. The GDPR is intended to have a horizontal application. The effects of the rules regarding the processing of data can have an impact on various areas of laws, such as public law, commercial law, employment law, but also contract law[82]. Therefore, the free character of the consent of the individuals purchasing a digital content is to be assessed on the basis of data protection law, as provided in the GDPR, applicable a of 25 May 2018, or in the Directive 95/46 and the e-Privacy Directive or the future e-Privacy Regulation once adopted.

64. A processing may also take place when it is necessary for the purposes of the **legitimate interests pursued by the controller or by a third party[83]**. In this case, a balancing exercise has to be performed between the legitimate interest pursued by the controller and the fundamental rights and freedoms of the data subject. The way to conduct this assessment is described in Recital 47 which suggests a strict interpretation. The Article 29 Working Party provided an Opinion in this regard, and already considered that processing data for marketing activities may constitute a legitimate interest[84]. Recital 47 explicitly mentions direct marketing as a potential legitimate interest. However, as for the assessment of the validity of the consent, the balance exercise relating to the legitimate interest of the controller or of third parties is a case-by-case analysis. Furthermore, the Court of Justice already stated that the data subject's fundamental rights override, as a rule, the economic interests of an operator[85]. Moreover, the legal basis of consent is more protective for the consumer than the use of legitimate interest[86]. One should note that the characteristics of the uses of data in the digital environment should as a rule of thumb require a free, specific, informed and unambiguous 'opt-in' consent[87] (as opposed to another legal ground such as the legitimate interests of the controller).

65. A processing may also take place on the basis of Article 6 (1) (c) of the GDPR, when the processing is necessary for **compliance with a legal obligation to which the controller is subject**. In order to link Article 3 (4) with the legal grounds for the processing of data, the purpose of ensuring that the digital content is in conformity with the contract or for meeting legal requirements (such the obligation to register the users) could therefore be considered as processing performed on this legal ground.

66. **For all these reasons, the Proposal should state explicitly that data processed by the suppliers shall only be used insofar this is in line with the EU data protection framework, including the GDPR and the e-Privacy legislation.**

3.3. The withdrawal of consent

67. The question of the freedom to withdraw one's consent is inextricably linked with the issue of free consent. Indeed, if a consent is considered as free when it is given as a legal ground for the processing of data, it should also be easily withdrawn without constraints. This principle is also stated in the e-Privacy Directive at Articles 6 (3) and 9 (3)-(4)[88]. The GDPR also provides clearly that *"The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent"*[89].

68. The conditions under which the withdrawal of consent can take place should be identical to the conditions under which the consent is considered as freely given. The free character of consent should indeed be assessed in the context of the provision of the consent, but also at the moment when such consent is withdrawn to preserve the systemic approach towards consent. The consequences of the withdrawal of the consent may imply the termination of the services, on condition that consent was already considered as free when it was provided to the supplier.

69. Moreover, the value generated by the supplier with the personal data of the consumer has usually already been created before the withdrawal of consent. The lawfulness of such a processing of data performed before the withdrawal shall not be affected by the withdrawal, according to Article 7 (3) of the GDPR.

70. The EDPS therefore recommends avoiding any additional provision on the contractual consequences of the withdrawal of consent that might be introduced by the Proposal and which would restrict the free choice of the data subject and his/her right to withdraw his/her consent.

3.4. The rights to access one's data and the right to portability

71. The present section will analyse how the GDPR interacts with Articles 13 and 16 of the Proposal (regarding the obligation of the supplier to refrain from using the data and the right of the consumer to retrieve his/her data).

a) The rights to object, erasure, object and the right to data portability

72. The Data Protection Directive provides that data shall be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"(Article 6.1.e).* Moreover, the Directive also provides for the right of the individuals a "**right of erasure**", which gives them the right to request *"as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive"*[90]. The Directive also provides for a **right to object**, under Article 14, according to which *"the processing instigated by the controller may no longer involve those data"* when the individual objected on compelling legitimate grounds and when the processing is based on the legitimate interests of the controller or of a third party[91]. When the purpose of the processing is direct marketing, the individual

does not need to demonstrate compelling reasons[92]. An example of the articulation between these principles can be found in the Google Spain decision of the Court of Justice[93].

73. These rights have been enhanced in the GDPR, notably with regard to the **right to erasure**, also called "**right to be forgotten**"(Article 17) especially when "*the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed"* and where *"the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing"*[94].

74. The **right to access** one's data, provided in Directive 95/46 under Article 12[95] has been confirmed and further developed by the GDPR in Article 15 Moreover, Article 21 of the GDPR introduces the "**right to data portability**" [96].

b) Interaction with the Proposal

75. As a preliminary remark, the EDPS reminds that it is likely that all or almost all the data concerned by Article 13 and 16 of the Proposal are to be considered as personal data. The same can said about the "*any other data collected by the supplier in relation to the supply of the digital content*" and "*any other data produced and generated through the consumer's use of the digital content to the extent that data has been retained by the supplier*", which are the terms used in the Proposal. Therefore, the obligation to stop the processing of "other data" might still be an added value for the consumer, as long as non-personal data might be processed by the suppliers concerned by the Proposal.

76. The Proposal provides for very similar obligations when it comes to **the obligation to stop the processing of data**. This similarity can be source of confusion since the scope of Articles 13 and 16 of the Proposal overlap with the relevant articles of the GDPR concerning the different rights at stake, but are also broader in terms of scope. For example, under data protection law, the controller of personal data must stop the processing of data as soon as these are not no longer necessary for the purpose of the processing. The wording of Article 13 and 16 seems to imply that the controller has to stop the processing of data on a best efforts basis, while the Directive 95/46 and the GDPR provide for an obligation to stop the processing and delete all the data concerned. Furthermore, the text of the Proposal excludes the data that were not provided as a counter-performance, while the Directive 95/46 and the GDPR apply to all data, irrespective of their use. For these reasons, the obligation to terminate the processing under the Proposal does not add much to the data protection principles.

77. Regarding **the right to retrieve one's data** in the Proposal, it is also very similar to the right to data portability and the rights of access. Article 15 of the GDPR indeed provides for the **right of access**, which entails the right to receive a copy of all personal data processed by the controller. This provision of the GDPR shall apply to any processing, including cases where no contract relationship exists, and without considerations pertaining to the use of data. Moreover, the information shall be provided for free[97] and *"in a commonly used electronic form",* while the Proposal provides that the consumer shall retrieve the content free of charge, *"and in a commonly used data format".* Therefore, all data provided and generated by the

supplier and which are personal data, shall be subject to the right to access under the GDPR, and the Proposal provides for a very similar right to the consumer. The **right to data portability** introduced by Article 20 of the GDPR goes even further since it gives the right to retrieve one's data *"in a structured, commonly used and machine-readable format"* but also to *"transmit those data to another controller without hindrance"*[98]. However, this right only applies when the processing is based on consent of if necessary for the performance of a contract, and only applies to personal data concerning the individual *"which he or she has provided to a controller"*.

78. **For these reasons, and in order to avoid confusion, the EDPS recommends that Articles 13 and 16 of the Proposal refer to the GDPR when it comes to the rights to erasure and the right to access one's data, to the extent that personal data are concerned. Should non-personal data ("other data") be processed, the EDPS recommends that the provisions of Article 13 and 16 should be aligned with the regime provided in the GDPR for the sake of consistency.**

CONCLUSION

79. **The EDPS welcomes the initiative of the Commission which intends to give a broad protection to consumers in the EU, by extending this protection to "digital goods", and by including the cases where consumers do not pay a price with money.**

80. **The EDPS recognises the importance of having clear and up-to-date rules which can accompany and foster the development of the digital economy. In this respect, the EDPS continues to follow actively the initiatives of the Commission regarding the Digital Single Market since the importance of data as a source of growth and innovation is at the core of these initiatives.**

81. **In this context, we welcome the initiative of the Council to consult the EDPS. This is for the EDPS an opportunity to address several recommendations and messages to the legislators, when discussing the Proposal submitted to the EDPS.**

82. On the interplay of the Proposal with data protection law:

- **the Proposal raises a number of issues given the fundamental rights nature of these data and the specific protection granted to these data under the EU data protection framework;**
- **the Proposal should avoid including provisions which may impact the data protection framework, since the Proposal is based on Article 114 TFEU, which is no longer the appropriate basis to regulate data processing;**
- **by no means should the Proposal change the balance found by the GDPR regarding the circumstances under which the processing of personal data may take place in the digital market.**

83. On the use of data as a counter-performance:

- **the EDPS considers that the term "data as a counter-performance" should be avoided;**
- **to this effect the EDPS offers alternatives:**
    - **the use of the notion of "services" in EU law may be useful in considering how to encompass services where a price is not paid;**
    - **the GDPR scope covering the offering of goods and services irrespective of whether a payment is required may also be a useful consideration.**

84. On the interplay of the Proposal with the GDPR:

- **considering the broad definition of personal data, it is likely that almost all data provided by the consumer to the provider of the digital content will be considered as personal data ;**
- **the EDPS recommends avoiding referring to data (actively) provided by the consumer since it contradicts the existing and future rules on data protection ;**
- **the Proposal should state explicitly that data processed by the suppliers shall only be used insofar this is in line with the EU data protection framework, including the GDPR and the e-Privacy legislation ;**
- **the EDPS recommends that Articles 13 and 16 of the Proposal refer to the GDPR when it comes to the rights to erasure and the right to access one's data, to the extent that personal data are concerned. Should non-personal data ("other data") be processed, the EDPS recommends that the provisions of Article 13 and 16 should be aligned with the regime provided in the GDPR for the sake of consistency.**

Brussels, 14 March 2017

(**signed**)

Giovani BUTTARELLI

European Data Protection Supervisor

Notes

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 119, 4.5.2016, p. 1.
[3] OJ L 8, 12.1.2001, p. 1.
[4] Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, COM/2015/0634, Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1450431933547&uri=CELEX:52015PC0634.
[5] Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, COM/2015/0635 final.
[6] For more information, see http://ec.europa.eu/justice/contract/digital-contract-rules/index_en.htm.
[7] In this context, an attempts was already made by the Commission: see Proposal for a Regulation of the European parliament and of the Council on a Common European Sales Law, COM/2011/0635 final; this proposal was abandoned by the Commission.
[8] Available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-582.370%2b03%2bDOC%2bPDF%2bV0%2f%2fEN.
[9] Available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-592.444%2b01%2bDOC%2bPDF%2bV0%2f%2fEN.
[10] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, p. 64–88.
[11] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29–34.
[12] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.
[13] See Explanatory Memorandum of the Proposal, page 3.
[14] See Article 3 (1) of the Proposal.
[15] See Article 13 (2) (c) of the Proposal.
[16] See Article 13 (2) (b) of the Proposal.
[17] See Article 3 (1) and (4), Article 13(2) (b), Article 15(2)(c) and Article 16(4)(a) of the Proposal.
[18] See Article 3(4) of the Proposal.
[19] Article 13(2) (b) and Article 16(4) (b) of the Proposal.
[20] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.
[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
[22] Article 3 (8) of the Proposal.
[23] Currently, in the context of the analysis of the Proposal, the main texts applicable are the Directive 95/46/EC which will be repealed and replaced by the Regulation (EU) 2016/679, and the 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), OJ L 201, 31.7.2002, p. 37–47 (also called "e-Privacy Directive"). The e-Privacy Directive should be repealed by the recent 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, 10 January 2017, COM (2017) 10 final (Regulation on Privacy and Electronic Communications).
[24] See communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions, "Towards a thriving data-driven economy", COM (2014) 442 final.
[25] See for example the Preliminary Opinion of the EDPS on "Privacy and competitiveness in the age of big data: The interplay between data protection , competition law and consumer protection in the Digital Economy", March 2014, available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf, and Opinion 8/2016 of the EDPS on coherent enforcement of

fundamental rights in the age of big data, 23 September 2016, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Events/16-09-23_BigData_opinion_EN.pdf.

[26] EDPS 08/2016 Opinion on coherent enforcement of fundamental rights in the digital age of big data of 23 Septembre 2016, page 6.

[27] Popular catchphrase like "digital currency" and "paying with data" may not only be misleading, but can also be dangerous, if it is taken literally and turned into a legal principle.

[28] See Article 29 Working party Opinion 03/2013 on purpose limitation, 2 April 2013, pages 10-11.

[29] See Section 3.

[30] See Recitals 2, 5, 7, 13, 21, 123, and 133.

[31] The notion of the "centre of gravity" has been developed by the ECJ. Where a measure may be adopted on more than one legal base, its main objective or component must be determined, see e.g. C-376/98, C-42/97, C-300/89. According to the settled case-law of the CJEU, *"the choice of legal basis for a Community measure must rest on objective factors (...), including in particular the aim and the content of the measure". In case of the GDPR, it cannot be contested that this so-called "centre of gravity"* is the protection of personal data. It is however not excluded that the GDPR may impact other EU objectives, such as the internal market, and therefore impact contractual law.

[32] See Recital 7 of the GDPR.

[33] See Recital 7 of the GDPR, *in fine.*

[34] See Article 3(8) of the Proposal, according to which the Directive "*is without prejudice to the protection of individuals with regard to the processing of personal data"* and Recital 22 of the Proposal which states that "*The protection of individuals with regard to the processing of personal data is governed by Directive 95/46/EC of the European Parliament and of the Council and by Directive 2002/58/EC of the European Parliament and of the Council which are fully applicable in the context of contracts for the supply of digital content. Those Directives already establish a legal framework in the field of personal data in the Union. The implementation and application of this Directive should be made in full compliance with that legal framework".*

[35] See Article 3 (4) of the Proposal: "*This Directive shall not apply to digital content provided against counter-performance other than money to the extent the supplier requests the consumer to provide personal data the processing of which is strictly necessary for the performance of the contract or for meeting legal requirements and the supplier does not further process them in a way incompatible with this purpose. It shall equally not apply to any other data the supplier requests the consumer to provide for the purpose of ensuring that the digital content is in conformity with the contract or of meeting legal requirements, and the supplier does not use that data for commercial purposes".*

[36] Preliminary Opinion of the EDPS on "Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy", already mentioned, n°80.

[37] See Preliminary Opinion of the EDPS on « Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy », already mentioned, n°77.

[38] See *i.e.* the German investigation into Facebook's possible abuse of market power by infringing data protection rules, mentioned in the EDPS Opinion 8/2016, page 13.

[39] As it is provided in the Proposal, see Articles 12 and 13.

[40] According to Article 57, *"Services" shall in particular include:*
(a) activities of an industrial character;
(b) activities of a commercial character;
(c) activities of craftsmen;
(d) activities of the professions."

[41] See CJUE, C-352/85, *Bond van Adverteerders and Others vs. The Netherlands State*, 26 April 1988.

[42] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16. The definition of information society service already exists in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services and in Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access; this definition covers *"any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service".*

[43] See Explanatory Memorandum of the Proposal, p. 3.

[44] Proposal of the Commission of 14 September 2016 for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (recast), available at https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-590-EN-F1-1.PDF. The proposed revision of

the EECC states in its Recital 16 that "*In order to fall within the scope of the definition of electronic communications service, a service needs to be provided normally in exchange for remuneration. In the digital economy, market participants increasingly consider information about users as having a monetary value. Electronic communications services are often supplied against counter-performance other than money, for instance by giving access to personal data or other data. The concept of remuneration should therefore encompass situations where the provider of a service requests and the end-user actively provides personal data, such as name or email address, or other data directly or indirectly to the provider. It should also encompass situations where the provider collects information without the end-user actively supplying it, such as personal data, including the IP address, or other automatically generated information, such as information collected and transmitted by a cookie)".*

[45] See Recital 14 of the Proposal.

[46] WP 29 Opinion 4/2007 on the concept of personal data, WP 136.

[47] Moreover, the fact that the data are those provided actively by the consumer implies that they are in principle related to him/her.

[48] Even to a greater extent, since Article 13 (2) (c) does not only apply to personal data provided to the supplier but also to all data generated through the consumer's use of the digital content.

[49] See Recital 13 of the Proposal: *"In the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money. Digital content is often supplied not in exchange for a price but against counter-performance other than money i.e. by giving access to personal data or other data. Those specific business models apply in different forms in a considerable part of the market. Introducing a differentiation depending on the nature of the counter-performance would discriminate between different business models; it would provide an unjustified incentive for businesses to move towards offering digital content against data. A level playing field should be ensured. In addition, defects of the performance features of the digital content supplied against counter-performance other than money may have an impact on the economic interests of consumers. Therefore the applicability of the rules of this Directive should not depend on whether a price is paid for the specific digital content in question."*

[50] Recital 14 of the Proposal excludes several categories of data such as IP address, cookies, but also location data, which are not actively provided by the consumer.

[51] See for example Article 29 Working Group, Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, WP 17.

[52] Article 29 Working Party Guidelines on the right to data portability, WP 242. This Opinion was subject to consultation and for comments until 15 February 2017.

[53] See Article 5(3) of the e-Privacy Directive.

[54] Proposal for an e-Privacy Regulation, Articles 6 and following.

[55] See also Article 6 of the Directive 95/46.

[56] Article 29 Working Party Opinion 03/2013 on purpose limitation, WP 203.

[57] See Article 6 (4) of the GDPR. As stated in this provisions, a further use of data is allowed on the basis of consent or on the basis of Member State or Union law "*which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 (1)"* of the GDPR.

[58] Article 6 of the GDPR provides that:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[59] As stated in the Article 29 Working Party Opinion 15/2011 on the definition of consent, WP 187, "*The choice of the most appropriate legal ground is not always obvious, especially perform a contract, or in order to take steps at the request of the data subject prior to entering into a contract, and no more. A data controller using Article 7(b) as a legal ground in the context of the conclusion of a contract cannot extend it to justify the processing of data going beyond what is necessary: he will need to legitimise the extra processing with a specific consent to which the requirements of Article 7(a) will apply. This shows the need for granularity in contract terms. In practice, it means that it can be necessary to have consent as an additional condition for some part of the processing. Either the processing is necessary to perform a contract, or (free) consent must be obtained. In some*

transactions a number of legal grounds could apply, at the same time. In other words, any data processing must at all times be in conformity with one or more legal grounds. This does not exclude the simultaneous use of several grounds, provided they are used in the right context. Some data collection and further processing may be necessary under the contract with the data subject – Article 7(b); other processing may be necessary as a result of a legal obligation – Article 7(c); the collection of additional information may require separate consent – Article 7(a); still other processing could also be legitimate under the balance of interests – Article 7(f) ».

[60] See paragraph 45 *supra*.

[61] See Article 13 (2) (c) of the GDPR.

[62] See Article 13 (2) (d) of the GDPR.

[63] See Article 13 (2) (c) of the GDPR.

[64] Article 29 Working Party 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of the Directive 95/46/EC, p. 16.

[65] As stated in the Article 29 Working Party Opinion 15/2011 on the definition of consent, WP187, "*The choice of the most appropriate legal ground is not always obvious, especially perform a contract, or in order to take steps at the request of the data subject prior to entering into a contract, and no more. A data controller using Article 7(b) as a legal ground in the context of the conclusion of a contract cannot extend it to justify the processing of data going beyond what is necessary: he will need to legitimise the extra processing with a specific consent to which the requirements of Article 7(a) will apply. This shows the need for granularity in contract terms. In practice, it means that it can be necessary to have consent as an additional condition for some part of the processing. Either the processing is necessary to perform a contract, or (free) consent must be obtained. In some transactions a number of legal grounds could apply, at the same time. In other words, any data processing must at all times be in conformity with one or more legal grounds. This does not exclude the simultaneous use of several grounds, provided they are used in the right context. Some data collection and further processing may be necessary under the contract with the data subject – Article 7(b); other processing may be necessary as a result of a legal obligation – Article 7(c); the collection of additional information may require separate consent – Article 7(a); still other processing could also be legitimate under the balance of interests – Article 7(f) ».*

[66] See Article 7 of the Directive 95/46 and Article 8 of the GDPR.

[67] Article 29 Working Party Opinion 15/2011 on the definition of consent, WP187.

[68] According to the EDPS, *"This is precisely the case of cookie walls, which often oblige the user to consent to the use of third-party tracking cookies, which are not necessary to the performance of the service concerned"*: see EDPS preliminary Opinion 5/2016 of 22 July 2016 on the review of the e-Privacy Directive, p. 15.

[69] Opinion 06/2014 on the notion of legitimate interest, p. 46. See also the Eurobarometer survey already mentioned which states that "almost two thirds of respondents say it is unacceptable to have their online activities monitored in exchange for unrestricted access to a certain website (64%)": http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/76377.

[70]Consultation on the e-Privacy Directive and Eurobarometer, available at http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/76377. See page 55: *"Just over one quarter think it is acceptable for companies to share information about them without their permission, even if it helps companies provide new services they might like (27%), while more than seven in ten (71%) say this is unacceptable".*

[71] See Article 9 (1) of the Proposal for an e-Privacy Regulation.

[72] See Recital 42 of the GDPR.

[73] Article 29 Working Party Opinion 15/2011 on the definition of consent, WP 187, p. 19.

[74] This question has been addressed by the EDPS in his Preliminary Opinion on privacy and competitiveness in the age of big data, pp. 34-36.

[75] See above, paragraph 50.

[76] See recital 43, first sentence of the GDPR.

[77] Opinion 06/2014 on the notion of legitimate interest, p. 46.

[78] In this respect, the EDPS recommended *"that the new provisions for e-Privacy further provide that irrespective of the market power of the service provider, it must (i) either provide a choice whether or not to provide consent to processing data not necessary for the provision of the service without any detriment, (ii) or at least, make available a paying service at a reasonable price (without behavioural advertising and collection of data), as an alternative to the services paid by users' personal information"*, see EDPS preliminary Opinion 5/2016, p. 15.

[79] EDPS preliminary Opinion 5/2016, p. 15.

[80] As an example of what should be considered as a free consent, the Working Party 29 mentioned the case of a social network where the users should be put in a position to give free and specific consent to receiving behavioural advertising, independently of his access to the social network service: see Article 29 Working Party Opinion 15/2011 on the definition of consent, WP 187, p. 18.

[81] Article 7 (4) jointly read with Recital 42 *in fine.*

[82] One can observe that Article 8 (3) of the GDRP states that the paragraph 1 of this Article *"shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child".* That means, *a contrario*, that the other provisions of the GDPR have an influence on contract law.
[83] See Article 6 (1) (f) of the GDPR.
[84] Article 29 Working Party, Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 25: *"controllers may have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalise their offers, and ultimately, offer products and services that better meet the needs and desires of the customers. In light of this, Article 7(f) may be an appropriate legal ground to be used for some types of marketing activities, on-line and off-line, provided that appropriate safeguards are in place (....). However, this does not mean that controllers would be able to rely on Article 7(f) to unduly monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from different sources that were initially collected in other contexts and for different purposes, and create - and, for example, with the intermediary of data brokers, also trade in - complex profiles of the customers' personalities and preferences without their knowledge, a workable mechanism to object, let alone informed consent. Such a profiling activity is likely to present a significant intrusion into the privacy of the customer, and when this is so, the controller's interest would be overridden by the interests and rights of the data subject".*
[85] CJEU, *Google Spain*, C-131/12, 13 May 2014, paragraphs 81, 97 and 99.
[86] For example, the right of withdrawal of consent under Article 7 (2) is more protective than the right to object; the right to data portability of Article 20 of the GDPR does not apply when the processing is based on legitimate interests, the conditions to obtain consent are more protective for the individuals since it requires an active action from his/her side.
[87] Opinion 06/2014 on the notion of legitimate interest, p. 47.
[88] See Also Article 29 Working Party Opinion on the definition of consent, p. 32.
[89] Recital 42 further develops the right of withdrawal by stating that "*Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".*
[90] Article 12 (b) of Directive 95/46.
[91] Or when the processing is *"necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed"*, see Article 14 (a) referring to Article 7 (e).
[92] See Article 14 (b) of Directive 95/46.
[93] CJEU, 13 May 2004, Google Spain, C-131/12.
[94] See Article 17 (1) (a) and (b) of the GDPR.
[95] According to this Article 12, the data subject has the right, among others, to obtain from the controller *"communication to him in an intelligible form of the data undergoing processing and of any available information as to their source"*.
[96] See Article 29 Working party Opinion on the right to data portability, WP 242, mentioned above. Article 20 of the GDPR states that:
"1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
(b) the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."
[97] Except for further copies requested, where the controller may charge a reasonable fee based on administrative costs.
[98] See Article 20 (1) of the GDPR.