Briefing
May 2017

European Parliament

# Contracts for the supply of digital content and personal data protection

**SUMMARY**

The proposed directive on the supply of digital content is intended to regulate the main contractual rights and duties of parties to contracts for the supply of digital content and services, and create a harmonised legal framework for digital content to benefit both consumers and businesses. It covers not only contracts where digital content or services are provided in exchange for money, but also those where the consumer provides personal or other data in lieu of money to gain access to digital content or services.

The interplay between this proposed private law instrument and the existing public law rules on data protection (notably the recently adopted General Data Protection Regulation) have been the subject of some debate. The European Data Protection Supervisor's recent opinion was critical of the proposal, arguing that, in the EU, personal data 'cannot be conceived as a mere economic asset' and cannot therefore be treated as the consumer's contractual counter-performance in lieu of money.

The draft report prepared by the co-rapporteurs in Parliament includes those contracts in which consumers do not pay a price (but potentially provide data) within the scope of the proposal. It eliminates however the notion of personal data as a form of contractual 'counter-performance'. The co-legislators are now facing the challenging task of reconciling the fundamental rights approach with the requirements of economic reality, including the need to grant legal protection to consumers who provide their data in order to access digital content or services.

**In this briefing:**



EPRS | European Parliamentary Research Service
Author: Rafał Mańko and Shara Monteleone
**Members' Research Service**
PE 603.929

## Introduction

In December 2015, the Commission submitted a proposal for a directive on the supply of digital content (hereinafter the DCD).[1] That directive, belonging to the field of private law, is intended to regulate the contractual rights and duties of businesses supplying digital content and providing digital services, on the one hand, and of consumers of such digital content and digital services, on the other. The proposal is designed to provide for maximum harmonisation[2] of key aspects of the contractual relationship, including conformity of digital content and services, termination of the contract by the consumer, and supplier's liability for damage caused to the consumer's digital environment.

The Commission claims the directive would contribute to faster growth of the digital single market (DSM) by creating a harmonised legal framework for digital content, benefiting both consumers and businesses.[3] This harmonised legal framework should, in the Commission's view, strengthen consumer trust when purchasing digital content and services online. Digital content is broadly defined in Article 2 DCD, and includes data produced and supplied in digital form (e.g. video, audio, applications and digital games); services allowing the creation or storage of data in digital form, where such data are provided by the consumer; and services allowing the sharing of data.

An important novelty of the proposed directive is that it covers, for the first time in EU law, contracts where digital content or services are supplied not only in consideration of a monetary price, but also in exchange **for the provision of personal data** or other data by the consumer. The stated reason for including contracts in which consumers make data available instead of paying a monetary price is the need to avoid discrimination between business models (recital 13 DCD). The relationship between this proposed private law instrument and the existing public law rules on data protection (notably the recently adopted General Data Protection Regulation) have been one of the focal points of debate on the DCD proposal.[4]

Within the Parliament, the proposal is being dealt with jointly by the Legal Affairs Committee and the Internal Market and Consumer Protection Committee. The co-rapporteurs, Axel Voss (EPP, Germany) and Evelyne Gebhardt (S&D, Germany) addressed the issue of data protection in their draft report of 7 November 2016. The Civil Liberties Committee, associated for opinion, focused its attention on the data protection aspects of digital contracts. A Coreper decision of 10 January 2017 requested that the European Data Protection Supervisor (EDPS) provide a written opinion on the data protection questions raised by the proposed directive. This was submitted on 14 March 2017. The Council's Legal Service has also presented an opinion on the interplay between the proposal and the data protection regime, but its substance has not been disclosed.

## The right to privacy and data protection in the EU

### Charter of Fundamental Rights and the Treaties

The protection of natural persons in relation to the processing of their personal data is a fundamental right enshrined in EU primary Law in Article 8 of the Charter of Fundamental Rights (CFR) and in Article 16 of the Treaty on the Functioning of the EU (TFEU). Article 16 TFEU, in particular, provides that the rules on the protection of individuals with regard to data processing by the EU and by the Member States acting within the scope of EU law are to be laid down following the ordinary legislative procedure. Article 8 CFR also states that personal 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*'. Article 7 CFR provides for the right to privacy, stating that 'everyone has the right to respect for his or her private and family life, home and communications'.

**European Convention on Human Rights**

Although the EU is not yet a signatory of the European Convention on Human Rights (ECHR) as provided for by Article 6(2) TEU, the ECHR remains, nonetheless, a source of general principles of EU law by virtue of Article 6(3) TEU. Furthermore, under Article 52(3) CFR, the meaning and scope of the fundamental rights guaranteed in the charter are to be given the same meaning as in the ECHR. Article 8 ECHR provides for a right of privacy. According to the case law of the European Court of Human Rights (ECtHR), the protection of personal data is a fundamental component of the right to privacy (*S and Marper* v *UK*, in the context of criminal justice). In *Airey* v *Ireland* the ECtHR held (in the context of family law) that whilst the right to privacy has essentially a vertical character (to protect the individual against arbitrary interference by the public authorities) it may also include a horizontal aspect (positive obligations on the state to ensure respect for privacy in relations between individuals). This applies also to the internet (*KU* v *Finland*).

**Secondary legislation**

These rules of EU primary law constitute the legal basis for EU secondary legislation on data processing. The main instruments of secondary European legislation are the Data Protection Directive (95/46/EC), to be replaced as of May 2018 by the 2016 General Data Protection Regulation (GDPR), and the e-Privacy Directive (2002/58/EC) (to be replaced by the proposed e-Privacy Regulation).

*The General Data Protection Regulation*

The GDPR contains general principles and rules that apply when entities in the private or public sector process personal data (e.g. on the conditions for processing, on the obligations and rights deriving from the data processing, and on necessary safeguards). It also aims to avoid unjustified limitations on the free flow of data. Accordingly, data processing activities are allowed under certain conditions, providing the persons retain their right to a private life, freedom of expression, and other rights.[5] The mandatory nature of the rules set out in the 1995 directive and the GDPR seeks to protect the fundamental rights to data protection and privacy in the *public interest*, as common goods, which, as some scholars put it, is necessary for the existence of a democratic society.[6] In practice, data protection law can be enforced by data protection authorities regardless of the data subject's will; sanctions for breach of those rules are mainly of an administrative (but can also be of a criminal) nature.[7]

This rights-based approach to data protection is closely related to self-determination and human dignity (as provided for in Article 2 CFR). From this perspective, personal data protection is treated as unalienable fundamental right rather than as a commodity that can be the object of exchange under a contract. This approach seems to prevail in the EU, while other (proprietary-oriented) approaches are taken, for instance, in the USA.[8]

## Personal data in the DCD proposal

**Monetisation of personal data as a business model**

While the EU Charter and ECHR treat personal data as a fundamental right of the individual, in economic reality businesses have quickly discovered that personal data can be easily monetised, and profit can be derived from their collection, processing and further sale. In fact, an entire business model has emerged in which personal data – having concrete economic value for companies – is being demanded from consumers wishing to access digital content or make use of digital services. This concrete economic reality has been taken into consideration by the Commission, which has proposed, in the Digital Content Directive, to grant protection not only to consumers who pay (with

money) for digital content and services, but also to those accessing to digital content and services upon supplying their personal data to businesses. Simultaneously, the proposal also seeks to grant consumers contractual rights relating to their personal data after the contractual relationship has come to an end.

**Personal data from a private law perspective**

Under European private law personal data are covered by the right of personality (*Persönlichkeitsrecht, droit de la personnalité*), and are therefore protected by a right effective vis-à-vis any third parties (*erga omnes*) that cannot be transferred. Nevertheless, they can be the object of a contract, for instance if famous actors allow their images and names to be used in advertisement campaigns, or if models agree, in modelling contracts, that their photographs can be published. In such cases the actor or model is not selling his or her image or name, but simply granting the business a contractual right to use that image or name, usually against remuneration. However, there seems to be no practice in the Member States' contract laws of treating the granting of the right to use one's personal data as a form of counter-performance (in lieu of monetary price).

**The notion of (personal) data in the proposal**

The DCD proposal refers to personal data in three contexts:

- (personal) data as the consumer's non-pecuniary counter-performance other than money (Articles 3(1), 13(2)(b), 15(2)(c) and 16(4)(a));
- (personal) data as data which is 'strictly necessary for the performance of the contract' (Article 3(4)), and is not therefore treated as the consumer's counter-performance;
- (personal) data 'as any other data produced or generated through the consumer's use of the digital content' (Articles 13(2)(b)-(c) and 16(4)(b)), which, in the proposal, becomes the object of the consumer's contractual rights once the contractual relationship is extinguished.

*Definition of (personal) data*

The original text of the proposed directive does not provide any definitions of 'personal data' relevant in this context. Neither does it specify what kind of data must be treated as 'strictly necessary' to perform the contract, or what is to be understood as 'other data produced or generated through the consumer's use of the digital content'. The proposed compromise amendment 1 to Article 2 DCD introduces a reference to the GDPR by including a definition whereby 'personal data' means personal data as defined by Article 4(1) of Regulation (EU) 2016/679'. The DCD proposal refers not only to 'personal data', but also to 'other data'. *A contrario*, the notion of 'other data' seems to refer to data that are not personal, which the consumer can pass on to the business. However, as the EDPS stressed in his recent opinion on DCD, the definition of personal data in the GDPR is broad enough to cover all the data mentioned in the DCD; the notion of 'other data' might therefore in practice turn out to be an empty one.

Another issue not included in the original DCD proposal (but included in amendments) is that of users' data being collected passively (or surreptitiously) by the digital content provider or other business (e.g. by using tracking cookies during website visits), enabling precise profiles of users to be put together for commercial or other purposes.

*Modifications suggested by the co-rapporteurs*

The original proposal covered contracts in which consumers *actively* provide personal data or other data as counter-performance, presumably to the trader (Article 3(1)). The rapporteurs would expand this definition to include data collected by the trader (i.e. provided passively by the consumer), as well as those collected by a third party 'in the

interest' of the trader. Under the original proposal, personal data 'strictly necessary for the performance of the contract or for meeting legal requirements' are excluded from the application of the same DCD, provided that the supplier does not further process it for other purposes. The rapporteurs would limit that exclusion to cover legal requirements only (Article 3(4)). Therefore, if the trader needs the data to perform the contract, but is not under a legal requirement to collect that data, the provision of that data – active or passive – will be treated as 'counter-performance' and bring the contract within the directive's scope.

## Interaction between the DCD proposal and the GDPR

### Mandatory nature of data protection rules

The GDPR as well as the e-Privacy directive (currently under review) seek to protect the individual's fundamental rights to data protection and privacy – in general (GDPR) and specifically in the context of electronic communications (e-Privacy directive).[9] It should be kept in mind that while the DCD is an instrument of private law (and seeks to harmonise private law rights and duties), the GDPR is an instrument of public law (seeking to protect the fundamental rights of individuals) and therefore its rules are mandatory (*jus cogens*) as opposed to being default (*jus dispositivum*). Therefore, data processed pursuant to contracts concluded under the DCD will also be subject to the GDPR, regardless of what the parties stipulate in the contract.

Hence, a contract for the supply of digital content or services will be subject to (at least) two distinct legal regimes, the private law regime of the Digital Content Directive (as implemented in national law) and the public law regime of the GDPR. This is not an unusual situation. The vast majority of economic relations *are* simultaneously subject to multiple legal regimes. For instance, a construction contract is subject to private law (as to the parties' rights and duties), but also to public law regimes of tax law (e.g. VAT rules), urban planning law, etc. The same applies to a simple sale of goods contract, which has not only private law implications, but is also subject to public law rules on VAT as well as any applicable public law rules (e.g. food safety), etc.

### Parallel application of distinct legal regimes to one transaction

That a contract for the supply of digital content will be subject to two distinct legal regimes raises the question of their mutual relationship. The proposed DCD states explicitly in Article 3(8) that the directive 'is without prejudice to the protection of individuals with regard to the processing of personal data'. Therefore, the relationship between the DCD and data protection law is not that of *lex specialis* – *lex generalis*, as contemplated in Article 3(7) for other private law instruments but, rather, one of parallel legal regimes.

The principle of *lex specialis derogat legi generali* (literally: 'a special law derogates from a general law') means that a legal norm having a narrower scope of application (the *lex specialis*) takes precedence, in case of conflict, over a legal norm having a broader scope of application (the *lex generalis*) that encompasses the scope of application of the *lex specialis*.

Moreover, the term 'is without prejudice' indicates that the DCD will not hinder, in any way, the exercise by the consumer/data subject of their GDPR rights vis-à-vis the business/data controller. It is important in this context that the GDPR is a public law instrument specifying the scope of a fundamental right, protected under the Charter. Another aspect relevant for the DCD is the scope of the concept of personal data (and its distinction from non-personal data), as this is an evolving technological era in which non-personal data may easily be transformed into personal data; the border between personal and non-personal data may be difficult to chart. However the GDPR (applicable to the first category) contains a definition (Article 4(1)) and it can be said that a broad

meaning of personal data applies.[10] This leads onto another point of discussion in the DCD proposal: its scope with regard to personal and *other data* (Article 3(1) DCD). As often clarified by the EDPS, metadata, the external data of communications, and also pseudonymous data are covered by the concept of personal data and thus by the GDPR. The concept of 'any other data' according to DCD has therefore still to be clarified.

**Consequences of violating the GDPR for the legality of the contract on digital content**

As indicated above, the DCD proposal does not impinge upon national 'general contract law'. The relevant rule of the DCD mentions, as examples, the rules on the validity and effects of contracts. Hence, the effects of a violation of a public law act (GDPR or national rules implementing the e-Privacy Directive) by the terms of a contract for the existence of the contract itself will depend on the applicable rules of each individual national system of private law. Such consequences can be diverse, ranging from voidness or voidability of the entire contract to voidness or voidability of the specific term, etc. This would lead to legal uncertainty and litigation with different outcomes not only across Member States but also between courts in an individual Member State.

The Parliament's co-rapporteurs wish to include a new rule (Article 4a) concerning contract terms detrimental to the consumer's data protection right under the 1995 Data Protection Directive, still in force, and the GDPR of 2016. Such terms would not be binding on the consumer, whilst the remaining part of the contract would continue to bind the parties if its terms were capable of existing without that unfair term.[11]

## Personal data as counter-performance

**Approach taken by the proposal**

According to Article 3(1) DCD, data provided by the consumer as 'counter-performance' in a contract for digital content can comprise 'personal data or any other data'. According to Article 3(4) DCD, the directive does not apply to personal data whose processing 'is *strictly necessary* for the performance of the contract' or 'for meeting legal requirements', provided that the supplier does not further process such data in a way incompatible with this purpose. Therefore, under the original proposal, personal data can be considered as a 'counter-performance' for digital content or services if it is provided *actively* by the consumer and such data are *not strictly necessary* either for the performance of the contract or for the supplier to meet legal requirements.

As clarified in recital 14 of the proposal, the *necessity* of data for the performance of the contract (the reason for the exclusion of these data from the application of the DCD directive) should be understood to mean necessity for the digital content to function correctly (e.g. geographic location data necessary for a mobile application to function properly, so as to provide a service for which data on the specific location are essential). By contrast, data provided, for instance, for registration purposes, or on the basis of a contract that allows access to user's data, would be subject to the DCD directive.[12] The provision on applicability of the DCD only to data *actively* provided by the consumer, meanwhile, seems to create discrepancies with data protection rules, which will apply in any case to data provided non-actively by consumers.[13] The only consequence of this would be to exclude from the DCD's scope of application all contracts in which personal data are collected without the consumer being aware of it (e.g. on website visits).

**Opinion of the EDPS**

The very idea of treating personal data as an object of contractual counter-performance has met with the opposition of the European Data Protection Supervisor (EDPS). In his

opinion of April 2017, while he recognised the importance of the data-driven economy for the growth of the EU and supported the aim of the DCD to ensure the protection of consumers who are required to disclose data as a condition for the supply of digital goods or services, he also warned against new provisions introducing the idea that people can pay with their data. He stressed that 'In the EU, personal information cannot be conceived as a mere economic asset. ... 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'. He also added that data protection rights 'cannot be reduced to simple consumer interests and personal data cannot be considered as a mere commodity'.

In order to avoid referring to data as counter-performance, the EDPS suggests two alternatives to delineate the scope of the DCD: a) the use of the notion of 'services' under TFEU (and as in the e-Commerce Directive) to include also services where a price is not paid; or b) using the terms of the GDPR, Article 3 (referring to the offering of goods and services irrespective of whether a payment of the data subject is required).

Regarding the possible interactions with the GDPR, the EDPS stresses that the broad definition of 'personal data' contained therein is likely to encompass almost all data covered by the DCD, including 'other data'; moreover, he notes that legal grounds for data processing are already laid down in the GDPR, including for processing data that are not necessary for the performance of a contract, which needs to be based on freely given consent (separate from the consent given to the contract's terms and conditions). Finally, the EDPS drew attention to possible overlaps and inconsistencies between the DCD and GDPR rules applicable in case of termination of the contract.

## Digital content contracts and the legal basis for data processing in the GDPR

### Overview of legal bases in the GDPR

The first issue to address with regard to personal data as counter-performance pursuant to the DCD is to identify under which legal basis, among those indicated by Article 6(1) GDPR, this data processing should be framed (to be considered legitimate under the data protection rules). Under this provision, there are three main legal grounds for data processing (out of a possible six) that could be relevant in the contractual context:

- consent given by the consumer (Article 6(1)(a) GDPR);
- 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 (Article 6(1)(b) GDPR);
- processing is necessary owing to the over-riding legitimate interests of the data controller.

### Requirement of free consent

It should be emphasised that Article 7(4) GDPR requires consent to be 'freely given', i.e. it should not be considered as a valid legal basis if it is conditional: this provision primarily aims to ban any pressure on a consumer's freedom of choice. Although it is not obvious how to interpret the concept of free consent, the aim of the high standard in Article 7 GDPR is to avoid precisely those situations in which the consent is not genuine, as the data subject does not have real choice.[14] Moreover, under Article 6(4), the GDPR does not rule out the processing of data without consent for a different, but compatible, purpose. Moreover, it must be noted that, regardless of the consent requirement (even

when it is not required and other legal grounds apply), the GDPR also recognises the right of the data subject to receive *information* about data processing, an aspect not addressed in the DCD proposal.

**Consent as legal basis for data processing**

Premise (a) of Article 6(1) GDPR concerns the consent requirement. Article 7 GDPR actually allows for the data subject to give consent 'in the context of a written declaration which also concerns other matters', provided that the consent is clearly indicated therein. Importantly, consent given under Article 7 may be withdrawn at any time (Article 7(3) GDPR), although the withdrawal has an *ex nunc* effect (i.e. from that point in time onwards), and data processing prior to it remains legal. Furthermore, Article 7(4) GDPR indicates 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'. It is clear that the consent to the contract for the provision of a service is conceptually and legally different from consent to data processing (and is to be indicated separately, e.g. in different clauses or boxes to tick). It seems also that personal data as 'counter-performance' under the draft DCD falls precisely within the scope of Article 7(4) GDPR, as the provision of access to digital content or digital services, under the DCD, is conditional on the processing of personal data that is 'not necessary for the performance' of the contract.

The DCD proposal is designed to grant rights to consumers under contracts in which traders do not require the payment of a price, but profit from their personal data.[15] The fact that data may have an economic value would not necessarily be an issue in terms of personal data protection as enshrined by the EU law, where, however, a **rights-based** approach prevails.[16] In other legal systems (especially in the USA) a different (proprietary) perspective of personal data, as asset at the free disposal of the consumer/owner of data, seems to prevail. The fact that most digital services and content are provided under the terms and conditions of US companies may be one reason for the tensions between these different legal approaches. However, EU policy-makers have been taking into account the economic aspects of data, and the profit that suppliers make from data, for decades,[17] without those aspects affecting the high level of data protection. Data protection has actually been strengthened in the GDPR and elsewhere.

Arguably, when a consumer provides data, e.g. to play an online game, this does not necessarily have to be seen, from a legal standpoint, as a synallagmatic contract (based on a *quid pro quo* exchange) within which a product or a service is exchanged *against* personal data (or against the obligation to consent to data processing).[18] A possible way of looking at the contract could be to see it as a gratuitous one, but subject to the fulfilment, by the consumer, of a public law condition, i.e. that the digital content is provided under the condition that the data subject consents to the processing of their personal data: consent that differs from that provided regarding the terms of the service (which remains within the contract). Consent to the processing of personal data would be covered by Article 6(1)(a) GDPR. As clarified by the Article 29 Working Party on Data Protection,[19] consent can be given *via* a conclusive action, like clicking a button (if this is clarified in the provider's notices).

**'Necessity for performance of contract' as a legal basis of data processing**

Article 6(1)(b) GDPR covers only data that are 'necessary for the performance of a contract' (i.e. without which the contract cannot be performed), hence personal data that are not necessary by definition escape the scope of this premise. It seems that data that are 'necessary' under Article 6(b) GDPR and data that are 'strictly necessary' for that

purpose under Article 3(4) DCD are, for all practical purposes, identical. Hence, if the consumer provides personal data on top of paying a price, and the data are '(strictly) necessary' to perform the contract, the business need not ask for additional consent – the contract as such will suffice for the purposes of the GDPR.

An additional open issue, is how to define, and who should define, what is 'necessary' to perform a contract for supply of digital content. However, if the consumer is asked (or encouraged) to provide personal data *other* than those '(strictly) necessary' for accessing the digital content, the business must – in order to comply with the GDPR – include in the contractual form a separate clause, concerning consent to the processing of these non-necessary data, that must fulfil the requirements set out in Articles 6(1)(a) and 7 GDPR.

**'Necessity for compliance with a legal obligation' as a legal basis for data processing**

At first sight, it might seem that a contractual obligation (under a supply of digital content contract) is a 'legal obligation' under Article 6(1)(c) GDPR, and therefore any data provided by consumers of digital content in the course of using the digital services would fall under that premise. However, contractual relationships have already been contemplated in Article 6(1)(b), and their repetition in point (c) would not make any sense. Instead, Article 6(1)(c) GDPR[20] is relevant for the purposes of applying Article 3(4) DCD as far as it coincides with the reference to 'data strictly necessary for meeting legal requirements'.

*Personal data provided as counter-performance*

In the case of personal data supplied by the consumer as a form of counter-performance in order to obtain access to digital content or services (e.g. to gain access to online movies or music seemingly 'for free'), it seems that this cannot be covered by Article 6(1)(b) GDPR (necessary to perform a contract) or else that would fall within the scope of Article 3(4) DCD and be excluded from its application, which would be contradictory. Therefore, consent is required (according to Article 6(1)(a) GDPR). In the case of personal data supplied by the consumer not as a form of counter-performance, but simply through using the digital content or service, paid for with money or not, it seems that such data, when necessary to perform a contract, could fall under Article 6(1)(b) GDPR, thus not requiring explicit consent. However, this would occur only if the processing of such data was actually covered by the terms of the contract. For instance, if a consumer has an account with a photographic social media platform which allows to upload and share photographs (including those which can be considered as personal data), it seems logical to claim that the operator of the platform has a duty to provide the service of processing and storing those data on its servers, of course subject to other public-law limits, in particular the 'purpose limitation' and 'data minimisation' requirements set out in Article 5 GDPR. In other words, no additional consent is required if the business processes personal data in order to fulfil its contractual duties to the consumer as a party to the contract (e.g. to provide tools for editing, storing and sharing photos).

It seems that data provided as counter-performance will always require additional consent (under Article 6(1)(a) GDPR), possibly added in the text of the contract as a separate clause, precisely because their processing is not necessary to *perform* the contract (as per Article 6(1)(b) GDPR).

*Additional data (not counter-performance and not strictly necessary)*

A third possibility in the context of a contract on digital content might be that data are provided not as counter-performance, nor are they a necessity for the contract's performance, but are (encouraged to be) provided on a voluntary basis (in addition to those requested 'in exchange' for digital content. For instance, in order to provide a

consumer with targeted advertisements separate consent is required (Article 6(1)(a) GDPR).

## Withdrawal of consent and termination

**Effect on the contract of a withdrawal of consent under the GDPR**

Under the GDPR, the data subject may, at any time, withdraw consent for data processing (Article 7(3) GDPR). Since the DCD is 'without prejudice' to the application of the GDPR, and owing to the primacy of the public-law rules of the GDPR over the DCD and the contractual agreement, the withdrawal of consent will be effective regardless of the private-law contract. As a result, the supplier will be under a duty (stemming directly from the GDPR) to stop processing the data collected from the consumer (which may not be used any more and in principle must be deleted). It could similarly be argued that, as a consequence of withdrawing consent, the service obtained in exchange for data as a counter-performance, such as downloading an application from the web, will also be (legitimately) stopped. This point of view relies on the approach to data as counter-performance that, as indicated above, the EDPS considers problematic under the GDPR. It also treats the granting of consent by the consumer as a fulfilment of the consumer's contractual obligation which has met with criticism from the Article 29 Working Party as not being in line with the approach of the data protection legal framework.[21]

The issue of withdrawal of consent is relevant only with regard to personal data that are *not necessary* for the performance of the contract (the latter data being covered by Article 6(1)(b) GDPR), and their processing therefore being lawful as a consequence of their necessity for the performance of a contract to which the data subject is party or because of legal requirements). For instance, in the case of an academic social media platform, users may be required to provide their affiliation and academic title (but not their photograph). If so, such data, necessary owing to the nature of the contract: (a) cannot be considered as counter-performance – thus it escapes the scope of the DCD; (b) does not require separate consent, as it is covered by Article 6(1)(b) GDPR. What is more controversial is the public-law status of data which are *not (strictly) necessary* for the performance of the contract and are supplied by the consumer to the trader either (a) as a form of 'counter-performance'; or (b) simply through using the digital service.

For instance, if a social media platform allows a free account to be opened and requires only the data that are necessary to run the account (again, the data necessary may differ from case to case), any other personal data supplied voluntarily (as optional) by the consumer will fall under this category. The question arises as to whether separate consent is needed in that case. This will be analysed separately, depending on whether they data fall under (a) or (b) above.

**Effects of termination of contract for data processing**

Terminating the contract, by virtue of the DCD (Article 16), has the effect of ending the supplier's right to use the consumer's data and of obliging the supplier to refrain from using the data in the future. It should be treated as a withdrawal of consent under Article 7(3) GDPR (with regard to data processed by virtue of consent), and also considered in accordance with the necessity and purpose limitation principles of the GDPR. Hence, a supplier of digital content who does not comply with their contractual duties of refraining from using the consumer's data on termination (Articles 13(2)(b) and 16(4)(b) DCD) would also be violating the GDPR, which may give rise to liability under Article 82 GDPR. The EDPS, in his opinion on DCD, claimed that the overlap between the DCD and the GDPR could generate confusion given the more stringent and precise obligations to stop (and delete) data under the GDPR. Indeed, Article 17 GDPR provides explicitly for the right to

erasure, also known as the right to be forgotten, whereby a data subject may require the data controller to erase personal data concerning the data subject without undue delay, inter alia when the data are no longer required or if the data subject has withdrawn consent.

*Consumer's right to retrieve data*

Another provision of the DCD proposal relevant to data protection is that entitling the consumer, in the event of termination of the contract, to retrieve all content provided (seemingly 'actively') by the same consumer or any other data produced or generated through the consumer's use of the digital content (Articles 13(2)(c) and 16(4)(b) DCD). This also seems to overlap with the GDPR (Article 20, right to data portability).

## Outstanding issues

A number of issues concerning personal data protection in the context of the DCD have still to be clarified, as they have not been addressed in the proposal. These include:

- methods for verifying if the business has actually stopped using the consumer's data after termination (Article 16 DCD) and the interplay with the rules of the GDPR concerning 'further processing of data' (Article 5(b), recital 50) and the right to be forgotten (Article 17 GDPR),
- access of the business to the consumer's digital environment (Article 9(3) and recital 33 DCD), which may include virtual access to the consumer's hardware – which entails a possible risk of the consumer's personal data being accessed,
- role of the business's privacy policy in ascertaining the conformity of the digital content or services with the contract; in particular, whether a publicly available privacy policy that promises protection higher than that required by the GDPR can be treated as part of the contract or at least as a criterion relevant for ascertaining the conformity of a business's performance with the contract.

## Conclusions

In terms of economic reality, the personal data of consumers have become a source of profit for businesses. This has enabled the emergence of an entire business model based on offering consumers digital content and services 'in exchange' for their economically valuable personal data, without requiring them to pay a separate price in money. In order to avoid discriminating between companies on the basis of the business model they opt for (digital content provided in exchange for money or after provision of their economically valuable personal data), the Commission proposes to include both types of situation/contract in the scope of the directive. This is also beneficial to consumers, as it grants them rights regardless of the method by which they get digital content and services – paying with money or providing personal data. However, at the same time the very idea of making personal data the object of a transaction has raised objections, including those of the European Data Protection Supervisor, based on fundamental rights concerns. The co-legislators now face a challenging task to reconcile the fundamental rights approach with the requirements of economic reality, including the need to grant legal protection for consumers who provide their personal data in order to access digital content or services. In addition, the final text must address the complex issues of the inter-relation between digital contract rules on the one hand, and personal data protection rules, on the other, in order to secure a transparent, coherent and workable legal environment for businesses and consumers in the digital single market.

## Main references

G. Spindler, 'Contracts For the Supply of Digital Content – Scope of application and basic approach – Proposal of the Commission for a Directive on contracts for the supply of digital content', 12 *European Review of Contract Law* 183 (2016).

R. Schulze et al. (eds.), *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps* (Nomos 2017).

## Endnotes

1 On the proposal see e.g. R. Mańko, *Contracts for supply of digital content: A legal analysis of the Commission's proposal for a new directive*, EPRS in-depth analysis, PE 582.048 (May 2016); idem, *Towards new rules on sales and digital content: Analysis of the key issues*, EPRS in-depth analysis, PE 599.359 (March 2017).

2 On maximum harmonisation see e.g. R. Mańko, The EU as a community of law: Overview of the role of law in the Union, EPRS briefing, PE 599.364 (March 2017), pp. 3-4.

3 Proposal for DCD, Explanatory memorandum p. 2

4 For references see: R. Mańko, Contracts for supply of digital content,, PE 599.310, pp. 9, 11.

5 For an overview, see EU Agency for Fundamental Rights, *Handbook on European data protection law* (2014); L.A. Bygrave, *Data Protection Law, Approaching its Rationale, Logic and Limits*, (Kluwer 2002).

6 A. Rouvroy, Y. Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in S. Gutwirth et al., *Reinventing Data Protection?* (Springer 2009).

7 For references see: D Le Metayer, S. Monteleone, 'Automated consent through privacy agents: Legal requirements and technical architecture', 25 *Computer Law & Security Review* 136 (2009).

8 See, inter alia, Paul M. Schwartz, 'Property, Privacy, and Personal Data', 117 *Harv. L. Rev*. 2055 (2004). For a conceptualisation of property rights in personal data in Europe, as legally possible, see N. Purtova, *Property Rights in Personal Data: a European Perspective* (Kluwer Law International, 2011), who, however, concludes that the property approach should not be ruled out in developing data protection.

9 See: L. Schrefler, Review of the ePrivacy Directive, EPRS Briefing Implementation Appraisal, 2017.

10 See also the EDPS's opinion on the DCD, p. 11.

11 This rule follows the model of the Unfair Terms Directive.

12 G. Spindler, op. cit.

13 As the European Data Protection Supervisor (EDPS) pointed out in his opinion on the DCD.

14 See Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13 July 2011. See also Information Commissioner's Office, ICO 2017 guidance (for public consultation).

15 Cfr. A. Acquisti et al. 'The Economics of Privacy', 52 *Journal of Economic Literature* (2016).

16 D. Le Metayer, S. Monteleone, op.cit.

17 See Commission Communication Towards a thriving data-driven economy (COM(2014) 442 final) and EDPS opinion on coherent enforcement of fundamental rights in the age of big data 8/2016.

18 See C. Langhanke & M. Schmidt-Kessel, Consumer data as consideration, 4 *Journal of European Consumer and Market Law* 218 (2015); F. Zoll, Personal data as remuneration in the proposal for a directive on supply of digital content in: R. Schulze et al (eds.), *Contracts for the supply of digital content: regulatory challenges and gaps* (Nomos 2017).

19 Opinion 15/2011, cit.

20 See GDPR (recitals 10, 31, 40 and 45).

21 See, among others, Article 29 WP Opinion 15/2011 on the definition of consent and EDPS opinion on DCD.

## Disclaimer and Copyright



eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)