THE COUPLING BAN IN DATA PROTECTION LAW – A FIRST APPROACH

Veronika Treitl

Veronika Treitl: Phd Assistant, Wien University of Economics and Business, IT / IP Law Group
Welthandelsplatz 1, 1020 Wien, AT
Veronika.Treitl@wu.ac.at; https://www.wu.ac.at/unternehmensrecht/institut/prof-winner-informations-und-immaterialgueterrecht/

Keywords: ***Data Protection Law, Coupling Ban, Consent, GDPR***

Abstract: *Consent to a data processing operation is only valid if it is freely given, demanding a genuine and free choice by the data subject. If, however, contract performance depends on consent to an unrelated processing operation (e.g. for marketing) a voluntary agreement is unlikely. The prohibition of coupling contract fulfilment to consent to a different data processing operation is regulated in Art. 7 para. 4 GDPR. While the essence of this «Coupling Ban» is sufficiently clear – it must be possible to decline the processing of personal data for other objectives than the contract but still enter into the contract itself – the succinct formulation of the Coupling Ban leaves room for legal interpretation.*

1. Introduction – Take it or leave it

Who has not experienced it: You want to order clothes in an online shop or subscribe[1] to a newspaper. Before you can conclude the contract, however, a text box in striking red font reminds you ever so nicely to agree to the usage of your personal information for marketing purposes, data transfer, and so on. Actually, you do not want others to use your data, yet you tick the box anyway as it is required to proceed. From thereon, you frequently receive e-mails from various companies informing you about special offers whatsoever. In the end, it is a *take it or leave it*[2] constellation where you can either choose to conclude the contract and accept data processing or refrain from the contract altogether.

Basically, such business practice is forbidden by European data protection law. Art. 7 para. 4 of the General Data Protection Regulation[3] (short: GDPR) stipulates that the fulfilment of a contract on part of the company must not depend on the data subject's consent to a different data processing operation. Although especially common, the approach of coercing people to superfluous consent declarations is not limited to online business. In fact, the Coupling Ban is also applicable in other situations where processing of personal information is required, as for example in employment relationships.[4]

The prohibition of coupling lacks a legal title. The *Article 29 Working Party* refers to it under the heading «*Conditionality»* and talks about «*bundling»* consent when describing coupling the performance of a contract with consent to an unrelated data processing operation.[5] Other terms used are the «*vertical restriction on*

---

1 DSB 22 May 2017, DSB-D216.396/0003-DSB/2017 discussed by Haidinger, Kopplungsverbot, Dako 2017, p. 92 (p. 93).

2 Buchner/Kühling in Kühling/Buchner, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 46.

3 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).

4 Tien, Online Bewerbungsverfahren: Umgang mit Bewerberdaten zur Begründung eines Beschäftigungsverhältnisses, Dako 2017, p. 88 (p. 89) with further references.

5 WP259 rev.01, Guidelines on Consent under Regulation 2016/679, pp. 7 f.

interconnection»[6] or simply the «*prohibition of coupling of consent»*[7]. With regard to linguistic clarity, this paper uses the term ***Coupling Ban***. The prohibition itself is already sufficiently complex and an unwieldy term would not help to improve clarification.

This paper, in which the Coupling Ban is addressed from an **online business perspective,** only offers a first approach to the subject. The hereby gained results shall form the basis for further research regarding other constellations where personal data are being processed.

2. Consent

The concept of consent is one of the key elements in data protection law. Consent constitutes the paramount expression of **informational self-determination**,[8] i.e. the sovereignty of natural persons over their data. Consent is the data subject's agreement to the processing of his or her personal information. Art. 4 para. 11 GDPR defines consent as a freely given, specific, informed and unambiguous agreement to the processing of the data subject's personal data. While all criteria are of relevance for evaluating valid consent, the **principle of voluntariness** is of paramount importance in the light of data protection law.[9] Although GDPR lacks a definition of voluntariness, Rec. 42 helps us with a negative distinction: «*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.»*[10] A detriment would then be any kind of (severe) disadvantage leading to a situation where the data subject feels obliged to agree to an unrelated data processing operation. This does not necessarily require physical coercion or threat of force but can be much subtler: A situation where the denial of consent entails additional costs or less favourable terms can pressure a prospective customer into giving consent.[11]

In this regard, the question arises whether **social pressure** can preclude the voluntary nature of a consent declaration. An example: Imagine your child attends kindergarten and the parents' association uses the messenger service WhatsApp to share relevant news about kindergarten activities. Without installing WhatsApp on your mobile phone, your access to information is complicated, if not impossible. If WhatsApp is the preferred means of communication by all the other parents, peer pressure requires you to participate. Thus, you feel urged to install this messenger service on your mobile phone, accepting the company's terms and conditions which include a comprehensive agreement to the processing of data stored on your mobile phone.[12]

If a data processing operation is based on consent, the respective declaration needs to fulfil the conditions for consent set out in Art. 7 GDPR. The prohibition of coupling is one of these conditions for valid consent (Art. 7 para. 4 GDPR). If a consent declaration violates one of the provisions set out in para. 1 to 4, the consent declaration is invalid. A processing operation based on an invalid consent declaration is unlawful. An infringement of the basic principles for processing, including the conditions for consent, may be subject to considerable administrative fines: 20,000,000 EUR or up to 4 % of the total worldwide annual turnover, whichever is higher (Art. 83 para. 5 lit. a GDPR).[13]

---

6 Dienst in Rücker/Kugler, A Practitioner's Guide, C.H. Beck, München 2018, Rz 448 distinguishes two restrictions on consent with regard to Art. 7 para. 4 and Rec. 43 GDPR. He defines the requirement for consent to an unrelated data processing operation as a «*vertical restriction on interconnection»* (Rec. 43, second half of the last sentence), as opposed to the «*horizontal restriction on interconnection»,* meaning that the controller must allow separate consent to be given to different personal data processing operations (Rec. 43, first half of the last sentence).

7 Eckert/Henschel, EU Data Protection - serious impact on Swiss companies. https://www.mme.ch/en/magazine/magazine-detail/url_magazine/eu_data_protection_serious_impact_on_swiss_companies/ (accessed on 4 January 2019).

8 Buchner/Kühling in Kühling/Buchner, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 19.

9 Heckmann/Paschke in Ehmann/Selmayr, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 45.

10 Rec. 42, last sentence.

11 WP259 rev.01, Guidelines on Consent under Regulation 2016/679, p. 11.

12 WhatsApp Security and Privacy https://faq.whatsapp.com/en/26000112/?category=5245250 (accessed on 5 January 2019).

13 Schulz in Gola, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 64.

3. What is the Coupling Ban?

It sounds simple enough: Consent to a data processing operation may not be voluntarily given if it is a prerequisite for entering into a contract for which the data processing is not necessary. In other words, the data subject shall be able to decline consent to a data processing operation which is dispensable for the performance of the contract but still enter into the contract itself. The Regulation addresses this prohibition in the legal text as well as in the Recitals.

3.1. Wording

According to Art. 7 para. 4 GDPR, «*[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract […] is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*». Rec. 43 GDPR, last sentence describes the same principle with a similar choice of words: «*Consent is presumed not to be freely given […] if the performance of a contract […] is dependent on the consent despite such consent not being necessary for such performance*». In both places, the provision of services is explicitly included. The Regulation does not distinguish between the conclusion and the performance of a contract as national law would.[14]

Following the wording of Art. 7 para. 4 and Rec. 43 GDPR it becomes clear that the prohibition of coupling is one important element of freely given consent[15] and can therefore directly affect the validity of a consent declaration. The point of reference is the necessity of a processing operation for the performance of a contract. The wording of Rec. 43 GDPR may be misleading here. The question is not whether **consent** to a processing operation is necessary for the performance of a contract but if the **processing operation itself** is necessary for the performance. Thus, the necessity of a processing operation is a **factual** requirement.[16]

Although the wording of Rec. 43 GDPR seems to suggest an extensive Coupling Ban,[17] the Regulation does not introduce an absolute[18] prohibition of coupling but demands that *utmost account* shall be taken to such contractual designs for assessing the voluntary nature of consent.[19] In other words, if the performance of a contract is subject to consent to another data processing operation, the consent declaration is not invalid per se. Rather, all the relevant **circumstances of the individual case** need to be assessed to evaluate whether it is indeed a situation of **unfair coupling**. The opinion of the *Article 29 Working Party* goes too far, claiming that these cases will be «highly exceptional».[20]

3.2. Scope of application

Data protection law is based on the **principle of prohibition**, reserving the **right of permission**.[21] This means that processing personal data is forbidden in principle, unless an exemption clause (Art. 6 para. 1 lit. a – f, Art. 9 para. 2 lit. a - j GDPR) is applicable. A data processing operation is, inter alia, lawful if it is based on valid consent (Art. 6 para. 1 lit. a GDPR for normal data or Art. 9 para. 2 lit. a GDPR as lex specialis[22] for sensitive data).

---

14 Feiler/Forgo/Weigl, GDPR: A Commentary, Globe Law and Business, Surrey 2018, Art. 7 Rz 8.

15 Kastelitz in Knyrim, Der DatKomm[3. Lfg], Manz, Wien 2018, Art. 7 Rz 33.

16 Dissenting Feiler/Forgo/Weigl, GDPR: A Commentary, Globe Law and Business, Surrey 2018, Art. 7 Rz 10.

17 The restrictive wording seems to reflect the initial draft of the European Parliament which was not adopted in the end. Kastelitz in Knyrim, Der DatKomm[3. Lfg], Manz, Wien 2018, Art. 7 Rz 34 FN 126 with reference to Gola, Neues Recht – neue Fragen, K&R 2017, p. 145 (p. 147) FN 18.

18 Arguing for a «*strict*» prohibition of coupling: Dammann, Erfolge und Defizite der EU-Datenschutzgrundverordnung, ZD 2016, p. 307 (p. 311).

19 Kastelitz in Knyrim, Der DatKomm[3. Lfg], Manz, Wien 2018, Art. 7 Rz 34 with further references.

20 WP259 rev.01, Guidelines on Consent under Regulation 2016/679, p. 9.

21 Frenzel in Paal/Pauly, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 6 Rz 1.

22 Schulz in Gola, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 6 Rz 14.

If interpreted strictly, the Coupling Ban forbids *bundling*[23] contract fulfilment with consent to an unrelated data processing operation. For determining such a situation of unfair coupling, it must be assessed whether the performance of a contract is conditional on consent to a processing operation which is not necessary for the performance of that contract. Argumentum e contrario, if the data processing is necessary for the performance of the underlying contract, coupling in the sense of a *take it or leave it-deal* would be allowed. The crux of the matter is, however, that a data processing operation necessary for the performance of the contract is lawful based on Art. 6 para. 1 lit. b GDPR. In this case, the controller does not need the data subject's agreement (Art. 6 para. 1 lit. a GDPR) as the processing is already allowed due to Art. 6 para. 1 lit. b GDPR.[24] So, if the data processing is necessary for the performance of the contract, the processing is lawful due to Art. 6 para. 1 lit. b GDPR and the data subject's consent is not required. Without a consent declaration, Art. 7 GDPR *(«Conditions for **Consent**»)* is inapplicable, as is the Coupling Ban. Only if the envisaged processing operation exceeds what is necessary for contract fulfilment, then consent is required and Art. 7 para. 4 applies again.[25] In the end, a contractual coupling clause would only be allowed in situations where the Coupling Ban is not applicable.

Although the exemption clause in Art. 6 para. 1 lit. b GDPR considerably diminishes the scope of application of the Coupling Ban, it is not eliminated: First, a controller can voluntarily choose to base its processing operation on a consent declaration, e.g. as a precaution in uncertain cases.[26] If the controller **chooses** the exemption of **consent** for processing personal information, then the Coupling Ban (and the other conditions stated in Art. 7 GDPR) must be adhered to.[27] Second, in the case of processing special categories of personal data listed in Art 9. para. 1 GDPR (e.g. racial or ethnic origin, political opinions, etc.) the exemption clauses of Art. 9 para. 2 GDPR instead of Art. 6 para. 1 GDPR are applicable. While both Articles allow a data processing operation based on consent, Art. 9 para. 2 GDPR does not provide an exception for a processing operation which is necessary for the performance of a contract. The consequence is that such **sensible data** must not be processed without explicit[28] consent given by the data subject, even if the fulfilment of the contractual obligation is otherwise not possible (given that no other exception of Art. 9 para. 2 lit. b – j is applicable).[29]

Yet, the strongest argument for the practical importance of the Coupling Ban lies in its conditional nature: The Coupling Ban is not an absolute one as Art. 7 para. 4 GDPR only requires that utmost account shall be taken of whether contractual designs include coupling.[30] Consequently, if the controller asks for consent for a data processing operation of normal personal data (precluding Art. 9 GDPR) and the processing operation is not necessary for the performance of the contract (precluding Art. 6 para. 1 lit. b GDPR) consent is **not per se invalid**. On the contrary, it can still be a situation of fair coupling considering the specific circumstances of each individual case.[31] But of course, the main difficulty lies in the identification and the assessment of these relevant circumstances.[32] Selected examples will be discussed hereafter.

---

23 WP259 rev.01, Guidelines on Consent under Regulation 2016/679, p. 9.

24 For a detailed elaboration see Engeler, Das überschätzte Kopplungsverbot, ZD 2018, p. 55 (p. 56).

25 Frenzel in Paal/Pauly, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 20.

26 Buchner/Petri in Kühling/Buchner, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 6 Rz 22.

27 For a discussion about the equal status of the individual exemption clauses see e.g. Schulz in Gola, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 6 Rz 10 ff.

28 For the processing of special categories of personal data based on Art. 9 para. 2 lit. a GDPR, consent needs to be given **explicitly,** precluding implied consent which would be sufficient under Art. 6 para. 1 lit. a GDPR; Weichert in Kühling/Buchner, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 9 Rz 47.

29 Kastelitz in Knyrim, Der DatKomm[3.Lfg], Manz, Wien 2018, Art. 7 Rz 37 with reference to Engeler, Das überschätzte Kopplungsverbot, ZD 2018, p. 55 (p. 58).

30 Heckmann/Paschke in Ehmann/Selmayr, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 53.

31 OGH 31 August 2018, 6 Ob 140/18h, no. 4.4.5, ÖBA 2018, p. 894 (p. 896). The Austrian Supreme Court stated that the controller needs to set forth the specific circumstances which would allow using a coupling clause in an exceptional situation.

32 Heckmann/Paschke in Ehmann/Selmayr, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 54.

3.3. Contractual Performance

According to the Coupling Ban, utmost account must be taken of whether the performance of a contract is dependent on the consent to a different data processing operation. Following the wording of Art 7. para. 4 GDPR and the purpose of the Coupling Ban – allowing freely given consent – one main assessment criterion for the Coupling Ban is the **necessity of the processing operation for contractual performance**. This leads us to two questions: (1) What is the performance of a contract and (2) when is the data processing operation necessary for such a performance?

3.3.1. Necessity and Characteristic Obligation

The *Article 29 Working Party* demands a strict interpretation of the criterion of necessity and requires a «*direct and objective link*» between the contractual performance and the processing operation.[33] Following this strict interpretation, *necessity* would mean that the fulfilment of the contract is not possible without the data processing. An example: If you order goods in an online shop your address must be processed, otherwise the delivery of the goods is not possible. The same must apply if the controller, e.g. an insurance company, bases its calculations for an individual contractual offer on the processing of the prospective customer's personal data.[34] A broader interpretation would result in the requirement of necessity to be already fulfilled if the data processing operation helps to **improve** the fulfillment of the contract in terms of costs, time or quality. An example: If you call the Austrian health hotline, medical staff answers your call and asks a series of questions to determine the need for medical treatment. If the staff had access to your full health record stored electronically, the evaluation of your medical problem could be faster and more accurate. The provision of the service – in this case providing medical information – is possible without processing your electronic health file, yet it would be more time and cost efficient and may provide better results.

Especially regarding the increased range of technologically advanced services, the minimum requirement for necessity could be the **economic feasibility** of an offer. If the controller cannot make an economically viable offer without processing the respective data, then the data processing is indeed necessary for the contract performance, at least in an economic sense. An example: A fitness center provides you with a smart watch that tracks your health data (sleep history, step counter, etc.) and transmits it to the company. Your fitness trainer then makes suggestions for a better life-style based on the results of the processing of your health data. Of course, it would be possible to talk to your fitness trainer face-to-face and provide him with the information (hours of rest, daily sports activities, etc.) personally. However, then the advantage of a standardized, well-tested, cost-efficient and fast processing program would be lost.

The criterion of necessity can only be evaluated in consideration of the performance of the contract. In order to assess whether a processing operation is related to the fulfilment of the underlying contract, the **characteristic obligation** of that contract needs to be identified.[35] In some cases, this is rather simple: When ordering goods, the performance is the delivery of the goods against payment. The usage of delivery details for marketing analysis would then be a different data processing operation.[36] For such traditional types of business transactions, the core of a specific contract can be determined according to the usual performance and counter-performance of the respective general contract type.[37] In other cases, especially with regard to new forms of contractual relationships, this approach may be too simplistic. For example, what is the characteristic obligation of the contract you have with a social media company or a search engine operator? Here, there are no (or only few) similar contracts whose usual characteristic obligation can be decisive for a necessity examination. Rather, the

---

33 WP259 rev.01, Guidelines on Consent under Regulation 2016/679, p. 8.

34 Buchner/Petri in Kühling/Buchner, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 47.

35 Buchner/Kühling in Kühling/Buchner, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 49.

36 Buchner, Informationelle Selbstbestimmung im Privatrecht, Mohr Siebeck, Tübingen 2006, p. 264.

37 Engeler, Das überschätzte Kopplungsverbot, ZD 2018, p. 55 (p. 57) calls this the «abstrakt-wertender Erforderlichkeitsmaßstab» which may be translated as *abstract necessity examination*.

specific contractual design needs to be evaluated in each individual case. It seems that this is the only way of considering individual and complex contracts appropriately.[38]

In the end, it is still unclear how to evaluate the necessity and the characteristic obligation of a contract. A restrictive approach would mean that a data processing operation in the sense of the Regulation is necessary only if contract fulfilment would not be possible without it. On the other hand, a broad interpretation would entail that the criterion of necessity is already fulfilled if the processing operation facilitates the performance of the contract. The threshold for necessity must probably lie somewhere in between these two interpretations, meaning that necessary processing operations should be more than just *useful* but need not be *indispensable* for contract fulfilment.[39] Thus far, it seems that the only consensus in legal literature is that the interpretation of the criterion of necessity is in fact a difficult one.[40]

3.3.2. Future field of research: Nothing is for free

The *Article 29 Working Party* argues that personal **data** shall not be given **in payment**, i.e. as a counter-performance. The agreement to the processing of personal information as a necessary consideration for the performance of a contract is presumed to be detrimental to freely given consent, thus violating the right of informational self-determination.[41] However, in many cases data processing is made part of the contract. Consider the **business model** of social media companies: They run a platform and allow users to sign up for it without paying any money. Rather, they generate revenue by selling all the personal information they collect when people use their platform (personal contacts, clickstream, political views, etc.).[42] This data normally exceeds what is necessary for running the platform on part of the company. Although users are not required to pay money for using the social network, they pay by giving away their data sovereignty. In fact, registering for a social media platform is usually advertised as **free-of-charge** and the information about data usage hidden in the small print,[43] while a separate consent declaration would be necessary. Though, consent can only be freely given if the data subject is aware of all the data processing operations included in the contract. Without being fully informed about the contractual content, data subjects cannot give valid consent (Art. 4 para. 11 GDPR). A lack of information can also lead to a violation of the principle of transparency (Art. 5 para. 1 lit. a GDPR).

A possible solution: Regarding the business model of social media companies, the characteristic obligation of the contract could be understood as a **barter trade**, where a service is provided in exchange for the usage of personal data.[44] The performance is the provision of a social network and the counter-performance is the permission for the commercial exploitation of the personal information gathered from the data subjects' usage of this platform. However, this would mean that the contractual definition of performance and counter-performance could circumvent the requirements for valid consent and thus endanger natural persons' data sovereignty.[45] The key aspect of this approach is that the prospective customers need to be informed in an intelligible way that they enter into a barter agreement (instead of entering into a cost-free service agreement). The **data trade** must be unambiguous and transparent,[46] enabling the data subjects to make an informed decision whether to enter into the barter agreement or rather refrain from the contract. In a functioning market with effective competition, the data subjects could then choose another company not coupling the data pro-

38 Engeler ibid. calls this the «konkret-objektiver Erforderlichkeitsmaßstab» which may be translated as *concrete necessity examination*.

39 Kazemi, GDPR, tredition, Hamburg 2018, Rz 148.

40 See for example Buchner, Informationelle Selbstbestimmung im Privatrecht, Mohr Siebeck, Tübingen 2006, p. 257.

41 WP259 rev.01, Guidelines on Consent under Regulation 2016/679, 9.

42 Frenzel in Paal/Pauly, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 21.

43 When registering for the social network Facebook, you are informed that Facebook is free and always will be; https://www.facebook.com/ (accessed on 5 January 2019).

44 Buchner, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, p. 155 (p. 158).

45 Golland, Das Kopplungsverbot in der Datenschutz-Grundverordnung, MMR 2018, p. 130 (p. 131).

46 Buchner/Kühling in Kühling/Buchner, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 51.

cessing to the provision of the service. The obvious problem lies in the existence of network effects:[47] You want to participate in a social network to stay in touch with your friends and family or simply to meet social expectations. Thus, you need to set up a profile with the same social network as the others. Participating in another social network would not meet your needs. The legal admissibility of business models that require data in payment for the performance of the contract is vividly discussed in legal literature and a common solution seems afar.[48] Indeed, further in-depth research is required.

3.4. Monopoly and reasonable alternatives

The strict adherence to the Coupling Ban constitutes an intervention with **freedom of contract**, as providers of goods and services are forbidden from using specific contract terms when it comes to data processing. The severity of this restriction may be softened if the Coupling Ban is only applicable in situations where the company occupies a **monopoly** position on the market.[49] With effective competition, prospective customers are able to compare alternative offers and may or may not choose a company which refrains from using data for dispensable purposes. Whichever their decision, they can act according to their free will. On the other hand, if a company occupies a monopoly position on the market, it can dictate the terms and conditions of the contract. The choice of consumers is then limited to either accepting the contractual content (including maybe excessive data usage) or refraining from the contract altogether (*take it or leave it*).[50] With respect to this limited scope of action, data subjects may feel pressured into giving consent if they want or need to conclude the contract.

In the light of data protection law, effective competition demands the existence of **reasonable alternatives**. This does not require an identical product or service at an identical price, but rather a comparable offer by the same or another provider.[51] Of course, a contractual agreement may be advantageous in terms of price or cutting-edge technology if it includes consent to an additional data processing operation.[52] An example: An online search engine provides you with more relevant results if it processes your personal data gathered from various sources (e.g. location data, previous searches, etc.). Conversely, the lack of such data processing may lead to increased costs for the customers or less advanced technology. Such an offer still constitutes a reasonable alternative as long as the disadvantages are not unreasonable.[53]

It is yet unclear in which cases the drawbacks of an offer are so severe that it does not present a reasonable alternative anymore. The assessment criterion could be the decision of a fictitious **average consumer**: Would he accept another offer as a reasonable alternative or dismiss it? An example: The Washington Post offers different types of subscription.[54] The basic one is for $ 60 a year with data being collected and sold to third parties. The premium subscription for $ 90 a year guarantees no on-site advertising or third-party tracking. With these alternative forms of subscription, prospective customers can choose whether to accept data usage or invest more money for ensuring privacy. Despite the increase in price, the premium subscription presents

47 Ibid. Rz 53 with reference to OLG Brandenburg 10 January 2006, 7 U 52/05.

48 See for example Buchner/Kühling in Kühling/Buchner, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 51; Engeler, Das überschätzte Kopplungsverbot, ZD 2018, p. 55 (p. 57); Feiler/Forgo, EU-DSGVO, Verlag Österreich, Wien 2017, Art. 7 Rz 11; Frenzel in Paal/Pauly, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 21; Golland, Das Kopplungsverbot in der Datenschutz-Grundverordnung, MMR 2018, p. 130 (p. 131).

49 Schulz in Gola, Datenschutz-Grundverordnung, C.H. Beck, München 2017, Art. 7 Rz 24. Dissenting Stemmer in Wolff/Brink, Datenschutzrecht, BeckOK, München 2017, Art. 7 Rz 44.

50 Buchner, Informationelle Selbstbestimmung im Privatrecht, Mohr Siebeck, Tübingen 2006, p. 265.

51 As the *Article 29 Working Party* judges coupling as highly undesirable, it does not see the existence of alternative offers by other suppliers as a sufficient justification for coupling; WP259 rev.01, Guidelines on Consent under Regulation 2016/679, p. 9 f.

52 Buchner, Informationelle Selbstbestimmung im Privatrecht, Mohr Siebeck, Tübingen 2006, p. 266.

53 This argument can be derived from previous German data protection law. Sec. 28 para. 3b BDSG provided a Coupling Ban regarding consent to data processing operations for advertisement and address trading; Plath in Plath, Kommentar zum BDSG und zur DSGVO^2, ottoschmidt, Köln 2016, § 28 Rz 170 ff.

54 https://www.washingtonpost.com/gdpr-consent/?destination=%2f%3f&utm_term=.5e47cfab4132 (accessed on 5 January 2019).

a reasonable alternative to the basic subscription. Differentiated offers are part of a company's contractual freedom.

It follows that the application of the Coupling Ban could be judged as being excessive in situations where a company is doing business in a functioning market. If there are several alternative offers for products and services (and some of them do not require unrelated data processing) the basic principle of data protection law – namely the right to informational self-determination – is upheld.[55] The inevitable follow-up question is, however, what happens if **all alternative offers** ask for **unrelated consent**? In such a situation, the prospective consumer is again in the dilemma that he must agree to an additional data processing operation if he wants to enter into any contractual relationship. Here, the Coupling Ban is indeed necessary to guarantee the principle of voluntariness. From an economic approach, this problem should resolve itself over time: If demand for privacy-friendly contractual agreements is strong enough, then supply will meet this requirement in the end. Though, respecting data privacy will most probably come at the expense of a higher price for goods and services charged by the supplier.

Considering the above, a company which wants to include a coupling clause in its contract terms would have to assess the existence of reasonable alternatives. If there is a single alternative offer available on the market which does not couple contract fulfilment to a superfluous consent declaration, including a coupling clause in its contract is lawful. However, it is then necessary to monitor the market consistently and adapt terms and conditions if the market situation changes.[56] The effort of observing the market could present an onerous burden for enterprises. A possible solution for a company would be to market two alternatives by itself: A cheap or free offer including a coupling clause, and a more expensive alternative without a coupling clause.[57]

4. Outlook

Much has been said about the Coupling Ban already. Yet we are still waiting for clear answers to several questions while others have not been addressed at all (e.g., Is the Coupling Ban only applicable when entering into a contract or also when an existing contract shall be modified? Do we have to consider lock-in effects and switching costs in case of already existing contractual relationships? Which rules apply for utility companies?). In the end, it will be left to the courts to shed light on the subject. Only recently has the Austrian Supreme Court refrained from the opportunity to refer a case regarding the Coupling Ban to the European Court of Justice.[58] It remains to be seen how high courts will decide about the Coupling Ban in the future.

---

55 Plath in Plath, Kommentar zum BDSG und zur DSGVO^2, ottoschmidt, Köln 2016, Art. 7 Rz 14.

56 Ibid. § 28 Rz 172.

57 Ingold in Sydow, Europäische Datenschutzgrundverordnung, Nomos, Baden-Baden 2017, Art. 7 Rz 33.

58 OGH 31 August 2018, 6 Ob 140/18h, no. 4.4.5, ÖBA 2018, p. 894 (p. 896).