

Compatibility as a Mechanism for Responsible Further Processing of Personal Data

Wouter Seinen, Attorney-at-law / Partner
Andre Walter, Executive Privacy Advisor
Sari van Grondelle, Attorney-at-law / Associate

Baker McKenzie Amsterdam N.V.
Claude Debussylaan 54, 1082 MD Amsterdam, Netherlands

Andre.Walter@bakermckenzie.com

Abstract. Further processing is probably one of the lesser researched features of the General Data Protection Regulation ("GDPR"). This is remarkable since much of the data to be processed involves data that was collected at an earlier stage and further processing is highly relevant for data controllers.

"Further processing" in this article refers to the processing of personal data for a purpose other than that for which it was initially collected. Article 6(4) of the GDPR provides the legal basis for such further processing. The key mechanisms are *consent* and a *compatibility assessment*.

Many privacy advocates consider consent to be the gold standard for further processing and pay little attention to the compatibility option. Consent, however, puts a significant cognitive load on individuals (the "data subjects"), while it confronts data controllers with serious challenges in obtaining consent and recording its validity. On the other hand, the compatibility assessment allows data controllers to justify the further processing based on the criteria given in Article 6(4), but it might leave individuals powerless.

In this article, we compare the two key mechanisms for further processing, consent and compatibility, and we discuss various compensating measures controllers can take to ensure that compatibility-based processing is a real alternative to consent.

Keywords: GDPR, personal data, data subjects, data controllers, consent, compatibility, privacy impact assessment

Introduction

"Further processing" of personal data gets little attention in legal literature. The General Data Protection Regulation (EU) 2016/679 (hereinafter the GDPR) provides legal grounds for processing and privacy principles that are at the foundation of the protection of personal data. Its principles define restrictions to the lawful use of personal data. For example, on the basis of the *principle of purpose limitation*, use of personal data shall generally be limited to the purpose for which the data was originally collected. In practice, further processing is highly relevant for most data controllers: they often have valid reasons to reuse data for further processing purposes. The GDPR provides the legal basis for such further processing in Article 6(4).

The key mechanisms to legitimate further processing under the GDPR require demonstrating (i) that such further processing takes place on the basis of *consent* or (ii) that a *compatibility assessment* demonstrates the compatibility of such further processing with the initial purpose.[1]

In this article we will assess whether the compatibility is an alternative to consent in guaranteeing a balance between the rights and freedoms of the individuals concerned and the interests of the data controller. We will analyze the privacy protection of the data subject in the situation of further processing by systematically comparing the two key mechanisms for further processing: consent and compatibility. We will address where the two mechanisms reveal deficiencies and discuss possible compensating measures that data controllers can take to ensure effective protection of personal data when processing data on a compatibility-basis.

We will look into (1) the general privacy principles, (2) the lawfulness of the initial processing of personal data, (3) the further processing of personal data, (4) consent as a mechanism for further processing, (5) compatibility as a mechanism for further processing, and we will provide (6) a comparison of the two key mechanisms of further processing. When discussing shortcomings of the data protection principles and data subjects' rights, we will also discuss potential compensating measures a controller might take to mitigate these shortcomings. In the conclusion (7) we will establish whether and when compatibility-based processing can be a real alternative to consent as a mechanism.

1 General Privacy Principles

Data protection is usually associated with the principles of proper data management, which include a number of requirements that must be imposed on the processing of personal data.[2] The importance of these requirements has been internationally accepted since the 1970s, and they are reflected in the general privacy provisions and principles in the GDPR: lawfulness of processing principle, transparency principle, fairness principle, purpose limitation principle, data minimization principle and storage principle. [3] [4]

As not all principles will be equally relevant for our comparison, we will only concentrate in this article on those principles that are directly related to the further processing of personal data.

2 Lawful Initial Processing of Personal Data

Article 5(1)(a) GDPR prescribes that the processing of personal data must always be lawful, fair, and transparent, where lawfulness requires one of the following processing grounds to apply:[5]

- a. the data subject has given consent to the processing of his or her personal data,
- b. processing is necessary for the performance of a contract,
- c. processing is necessary for compliance with a legal obligation,
- d. processing is necessary to protect the vital interests of an individual,
- e. processing is necessary for the performance of a task carried out in the public interest, or
- f. processing is necessary for legitimate interests pursued by the controller or by a third party.

In the case of processing on the basis of consent (ground (a)), the data subject is responsible for determining whether he or she believes that the processing activity envisaged is appropriate in the context of their interests (i.e., rights and freedoms). In case of the other legal grounds (grounds (b) through (f)), the data controller is the actor who needs to determine whether the processing activity envisaged is necessary and possibly outweighs the interests of the data subject.

From a business perspective, a controller should rely on consent only in cases where none of the other grounds apply. Consent is a very fragile concept; it can be withdrawn at any time by the data subject, and the validity of consent might be challenged by data subjects as well as by supervisory authorities. Moreover, consent-based processing comes with additional burdens for the controller such as extended data subject rights and the requirement to create an audit trail to prove that consent was obtained or withdrawn in a valid manner.

3 Further Processing of Personal Data

Despite the purpose limitation mentioned above, the GDPR provides an opening for further processing of data for purposes other than that for which the personal data have been initially collected.[6] This requires that the further processing is based on (i) the data subject's

consent, (ii) Union or Member State law, which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), or that (iii) the controller ascertains that the further processing is compatible with the initial purpose.

In the remainder of this paper, we will focus on the two key mechanisms of further processing: consent and compatibility. The aim of the paper is to understand the dynamics between controllers and data subjects and to assess their ability to take responsibility in the further processing in order to materialize a high standard of privacy and data protection.

We assume here that personal data initially collected on the basis of consent will have to be further processed based on consent. In its guidance on consent, the Working Party 29 (hereinafter: WP29) is of the opinion that if a controller wishes to continue processing the personal data on another lawful basis, it cannot silently migrate from consent to that other lawful basis.[7] Although the GDPR does not specifically mention ascertaining of compatibility as a lawful ground of processing in Article 6(1), expert opinions vary on this matter.[8]

4 Consent as a Mechanism for Further Processing

The first mechanism of further processing of personal data that we consider is consent. To obtain consent for further processing, the same requirements apply as in the case of consent for the initial collection. The GDPR requires obtaining consent by way of a clear affirmative act, establishing a freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement (including by electronic means) or an oral statement.[9]

Such information must ensure that the data subject is aware of the fact that consent is given and the extent to which it is given. For consent to be informed, the data subject should be aware, *inter alia*, of the identity of the controller and the purposes of the processing for which the personal data are intended.[10] Furthermore, consent may be given by the data subject for the processing of his or her personal data for one or more specific purposes. It shall cover all processing activities carried out, and when the processing has multiple purposes, consent shall be given for all of them.

Under the GDPR, whenever processing is based on consent, the controller is obligated to demonstrate that the data subject has consented to the processing of his or her personal data. Consent shall therefore be recorded in such a way as to provide evidence that, and show how, consent was given. This means that a controller shall implement an effective audit trail of the process deployed for obtaining consent and keep it up to date.

For the data subject, processing on the legal basis of consent means that he or she is in control and is responsible for determining whether the processing activity envisaged is appropriate and desirable with regard to their interests, rights, and freedoms. The data controller may ask consent for a processing activity and then leave the assessment of the appropriateness thereof to the data subject.

Finally, where the data subject has given consent for a specific further processing, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes.[11]

5 Compatibility as a Mechanism for Further Processing

The purpose limitation principle of the GDPR does not impose a requirement of compatibility; rather it prohibits *incompatibility*. [12] The European legislator intended to provide some flexibility regarding further processing. In a fast-moving world, this flexibility may be needed to allow for a change of scope or focus in situations where the business environment changes or expectations of the data subject and/or of the society at large change on the notion of what further processing may be appropriate and compatible.

Compatibility is not a straightforward concept. Compatibility of further processing purposes needs to be assessed on a case-by-case basis, and the data controller cannot legitimize incompatible processing by simply constructing a new lawful processing ground. Moreo-

ver, the GDPR states that, in such a case of further processing, no legal basis separate from that which allowed the initial collection of the personal data is required.[13]

After having met all the requirements for the lawfulness of the original processing, a controller should perform a compatibility assessment for further processing of personal data, considering, *inter alia*, the following factors:

- a. any link between the purposes for which the personal data have been collected and the purposes of the further processing intended;
- b. the context in which the personal data have been collected, in particular the reasonable expectations of data subjects, based on their relationship with a data controller, as to their further processing;
- c. the nature of the personal data, in particular whether special categories of personal data or personal data related to criminal convictions and offenses are processed;
- d. the possible consequences of the intended further processing for data subjects; and
- e. the existence of appropriate safeguards, which may include encryption or pseudonymization.

The compatibility assessment considers the five factors described above in order to establish whether the further processing may be considered compatible. An inherent characteristic of such a multifactor assessment is that shortcomings of certain factors may in some cases be compensated by better performance in other areas.[14] The performance of the five factors can therefore balance each other.

In practice, such an assessment cannot be regarded as an entirely quantitative assessment or a purely mathematical exercise, such as by simply averaging the scores assessed in the five categories. A qualitative judgment of the situation by a qualified legal or data protection expert is always recommended and often a necessity. Such an assessment should be documented and kept available for internal and external review by the privacy officer, an auditor, supervisory authorities, or even the data subjects concerned.

Besides this, the GDPR explicitly privileges further processing of personal data for historical, statistical, or scientific purposes, provided that Member States implement appropriate technical and organizational measures.[15] When there is compliance with the safety measures required, processing for these purposes is explicitly considered to be compatible.[16] The privileging rule covers a broad range of processing activities, such as purposes of public interests (e.g. medical research), as well as commercial purposes (e.g. analytical tools of websites or big data applications aimed at market research).[17] Member State laws may provide for additional situations that justify the further processing of personal data that was obtained for other purposes and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful.

6 Comparison of the Key Mechanisms of Further Processing

Many privacy advocates consider consent to be the gold standard for further processing and pay little attention to the compatibility option. Consent, however, puts a significant cognitive load on data subjects while it confronts data controllers with serious challenges in obtaining consent and recording its validity. Alternatively, the compatibility assessment allows data controllers to justify the further processing based on the criteria given in Article 6(4), but it might leave the individual powerless.

The two key mechanisms of enabling further processing of personal data – consent and compatibility – will be discussed below, and a complete overview of the comparison will be provided in Appendix 1. The comparison covers the three most important areas of materializing privacy protection: (i) the principles of personal data processing,[18] (ii) data subject rights and freedoms, and (iii) controller obligations and interests. We aimed for an objective comparison of how the two mechanisms of consent and compatibility perform in terms of privacy protection based on the legal requirements of the GDPR and the feasibility of implementation.

Initially, consent seems to be the better choice for living up to the principles of personal data processing and guaranteeing data subjects' rights and freedoms. In terms of feasibility of implementation, though, compatibility appears preferable. Table 1 in Appendix 1 gives

more insight into our considerations for this baseline assessment. In the section Summary of Compensating Measures, we will review possible improvement areas where compatibility falls short compared to the consent mechanism. Additional measures will be discussed that could improve performance to make it comparable with consent.

6.1 Data Protection Principles

The GDPR privacy principles and their importance for the protection of human rights and fundamental freedoms for data subjects have been mentioned in section 1 above. For some of the data protection principles, we identified no differences or only very limited differences (see Appendix 1): accuracy, integrity/confidentiality, and accountability.

Lawfulness of Processing Principles. As described in section 3 above, data initially collected by consent should not be further processed based on other lawful grounds. Although the GDPR language does not give clear guidance on this, we respect the view of the supervisory authorities on this point, and in further discussion below we exclude data that is initially collected on the basis of consent.[19] Further research will be needed to examine the current position taken by the supervisory authorities.

Transparency Principle. To live up to the transparency principle, the controller will have to provide a publicly available privacy notice that explains the purpose and modalities of the further processing. Using compatibility as a mechanism, the controller should also disclose the compatibility assessment methodology that has been applied in order to justify the further processing of the data.

As much of this information will appear complex to the data subject and to the broader public, the controller should strive for increasing transparency and reducing the cognitive load on the data subject. Information should be made easily accessible, using clear and plain language, and should be supported by visual means of presentation where possible and appropriate.

Further processing through consent requires presenting the data subject a just-in-time notice specifically focusing on the processing purpose envisioned. As this is generally not required for further processing based on compatibility, the controller should therefore consider providing additional transparency controls voluntarily. The WP29 coins the term *pull notices* for these transparency controls that provide data subjects access to additional information, and it specifically mentions methods such as privacy dashboards and “learn more” tutorials.[20]

Fairness Principle. Appendix 1 indicates a weakness of compatibility related to the fairness principle, because the controller makes the decision whether the purpose of the further processing is compatible with the initial purpose, while consent leaves this decision to the data subject. To become comparable with consent, the controller should provide additional features to compensate for this shortcoming, allowing data subjects to opt out of the further processing that has been deemed compatible by the controller. The options should be offered in a user-friendly and intuitive manner in order to get on an equal footing with consent. Withdrawal of consent has to be as easy as giving consent, and the WP29 adds that it must be possible to give and withdraw consent via the same interface.[21] Permission management systems would be a workable way to provide the additional choice and options features.[22]

Purpose Limitation Principle. Purpose limitation is relevant with regard to one specific element of the compatibility assessment, namely the link and distance between the purpose for which the personal data have been collected and the purposes of the intended further processing. The controller should be very transparent about the differences between these purposes and the distance between them, and should disclose the compatibility assessment methodology and policy decisions that apply to the operation at hand. Consent leaves this decision about the gap between the purposes to the data subject. Therefore, the controller making this decision based on compatibility should not leave the individual powerless and

should provide the data subject with tools allowing unconditional opt-out possibilities. To become comparable with consent, this should go further than just providing the “right to object.” In the “right to object” scenario, the controller can take his or her time to evaluate the objection and come up with compelling reasons to reject the request, weakening the data subject’s position.[23]

Data Minimization Principle. Data minimization is an important aspect in the pursuance of guaranty proportionality and necessity of the data processing. In applying the compatibility assessment, the controller is the actor who will determine proportionality and necessity. Based on the assumption that the compatibility assessment assures compatibility with the initial purpose but does not define a new lawful ground of processing, the GDPR provides the data subject the right to object to this decision only if the initial processing has taken place in the context of public interest or the controller’s legitimate interest. Moreover, as explained under the purpose limitation principle, the controller can reject the objection request under certain circumstances, risking leaving the individual powerless. Again, permission management features would be appropriate to reach comparability with consent.

Storage Limitation Principle. To live up to the storage limitation principle, compatibility needs additional measures to be comparable with consent. Although the principle that personal data shall be erased if no longer needed applies to all processing grounds, withdrawal of consent triggers the erasure process explicitly.[24] For processing grounds other than consent, the controller’s retention policy has to be applied. To become comparable with consent in this respect, here too a voluntary opt-out feature could be the solution to triggering the same erasure process as a consent withdrawal.

6.2 Data Subjects – Rights and Freedoms

The GDPR grants data subjects a range of specific data subject rights that they can exercise under certain conditions, with a few exceptions. Given the focus of supervisory authorities on these rights, GDPR compliance should specifically enable the exercise of these rights. Some data subject rights are independent of the lawful processing ground, including *data subject access* requests, the *right to restriction of processing*, and the *right to rectification*. For exercising these two rights, it makes no difference whether consent or compatibility is used as a mechanism for further processing of data. However, the exercise of some data subject rights depends on the lawful ground of the initial processing. This applies to the *right to erasure*, the *right to portability*, and the *right to object* to the processing of personal data concerning the data subject. We will now discuss how to come on an equal footing with consent for these rights.

Right to Erasure. The *right to erasure* (Article 17 GDPR) is triggered by consent withdrawal. For processing grounds other than consent, the controller’s retention policy has to be applied. To become comparable with consent in this respect, further processing via compatibility should provide a voluntary opt-out feature triggering the same erasure process as consent withdrawal.

Right to Portability. The *right to portability* (Article 20 GDPR) is only applicable for personal data that is provided by the data subject himself or herself, including data collected under consent and for the performance of contract. The right to portability is not applicable for other lawful grounds of the initial purpose. Therefore, the right to data portability applies to all personal data further processed based on consent, but it does not necessarily have to be provided for further processing based on compatibility. To compensate this shortcoming of compatibility, controllers could consider granting a voluntary data portability right for *all* data used for secondary purposes, when relying on compatibility.

Right to Object. The *right to object* (Article 21 GDPR) is generally only provided for processing that takes place in the context of the controller’s legitimate interest, direct marketing, or for processing in the public interest. However, in practice, the consent

withdrawal mechanism too gives unconditional objection power. Moreover, the GDPR requires this unconditional objection power *a priori* when data are used for direct marketing purposes.[25] It also raises the bar for processing purposes based on legitimate grounds, by obliging the controller to demonstrate *compelling* legitimate grounds to reject such an objection request.[26] To become comparable with consent, an effective mitigation measure would provide an unconditional opt-out feature for all processing purposes based on compatibility.

Choice and Options. Giving choice and options to data subjects to control their data is promoted by the GDPR as an objective.[27] The ICO, for example, is promoting consent as a “higher ideal,” stating: “Consent means giving people genuine choice and control over how you use their data.”[28] Conceptually this is right: giving and withdrawal of consent should provide the means for genuine choice, but the challenge lies in the practical implementation. Thoroughly implemented permission management systems providing user-friendly features for data subjects to exercise control over their data can realize this “higher ideal.” These systems could equally facilitate choice and options for both mechanisms: opt-in (consent) or opt-out (compatibility).

6.3 Controller Obligations and Interests

Generally, controller obligations and the provisions for transfers of personal data to third countries are independent from lawful grounds of processing.[29] [30] There are small nuances of data transfer derogations for specific situations, which will not be discussed in this article in further detail.[31]

Implementation and Continuity. Unlike for the data subject, the compatibility mechanism has many upsides for controllers compared to consent. The implementation and impacts are different. The compatibility approach works better for further processing activities with regard to continuing the processing operations. For example, although a data subject has the right to object to the processing, he or she cannot stop a processing immediately and unconditionally, with a few exceptions. With consent, the data subject can withdraw the consent at any time, unconditionally.

Profiling. Profiling is another purpose many controllers pursue. Collecting consent for profiling can be challenging for controllers because in such an early stage of analysis, data subjects do not see “what’s in it for them.” Further processing for profiling operations that pass the compatibility assessment could be performed without the consent of the data subject.

Special Categories of Data. Processing of this category of data is generally prohibited under the GDPR unless a number of specific exemptions apply.[32] [33] One of the exception grounds is *explicit consent*, which makes consent the preferred mechanism for secondary use of special categories of personal data, as referred to in Article 9(1). There are only limited exception grounds that lift the prohibition on further processing of special categories of personal data based on compatibility. Examples of this are, *inter alia*, processing in the employment context, for vital or substantial public (health/research) interests, and certain processing in the context of foundations, associations, or any other not-for-profit bodies.

6.4 Summary of Compensating Measures

Measures that can be used to compensate for the shortcomings of compatibility compared to consent are summarized and further elaborated below.

Pull Notices. Pull notices are suitable for providing additional transparency controls. They provide an additional layer of communication to the data subject over push notices which usually cover the information requirements laid down in the GDPR, typically referred to as

privacy notices or just-in-time information notices.[34] Typical implementation examples in practice are dedicated privacy portals, permission management that facilitates direct communication channels with the data subject, privacy dashboards, and “learn more” tutorials. Pull notices allow for a more user-centric transparency experience for the data subject.

Voluntary Opt-Out. Data subjects have the right to object to the processing of their personal data when it is based on legitimate grounds of the controller. The objection should reflect grounds relating to the data subject’s particular situation, and the processing should be stopped until the controller has demonstrated “compelling legitimate grounds” to continue. The WP29 has clarified that for legitimate interests to be considered compelling, a higher threshold is required than the lawful ground of legitimate interest as found in Article 6(1)(f) GDPR.[35]

The above highlights two important points. First, it should be possible to provide an opt-out from certain personal data processing based on the data subject’s particular situation. Second, there might be compelling reasons for the controller to pursue its legitimate interests despite the data subject’s objection. Thus there must be a range of *non-compelling* processing purposes where the controller should offer the data subject unconditional opt-out possibilities.

Current guidance and earlier investigations by supervisory authorities support the idea of providing voluntary opt-out possibilities to mitigate negative consequences for the data subject. The ICO, for example, states in the context of the legitimate interests assessment that it might be helpful to consider offering an opt-out to balance the interest of the controller with that of the data subject.[36] The Dutch DPA indicated the same in an earlier Wi-Fi tracking investigation.[37]

Permission Management. Permission management systems are typically personalized applications and are designed to assist their users to manage their permission settings in a transparent and user-friendly manner. These permission management systems should at least cover all further processing purposes in order to be an effective compensating measure. In the privacy context, these systems are sometimes referred to as “consent managers,”[38] focusing primarily on consent-based processing. These systems can typically manage the granting and withdrawal of consent, including the registration of it. Besides this, there are other concepts entering the privacy arena, for example *Customer Identity Access Management (CIAM)*. [39] [40] These systems are mainly driven from the marketing and logical access management side. *Personal information management systems (PIMS)* originated in a movement in society to give data subjects more ownership and control over their data.[41] These tools could offer effective mechanisms for objecting, such as a user-controlled opt-out feature.

Erasure Trigger. Erasure will have to be triggered at consent withdrawal. In practice this requires triggering the data retention process within the controller’s organization. For other processing grounds, the controller could implement a similar erasure trigger that activates the retention process in the same way as consent withdrawal would. A straightforward practical solution could be to initiate that trigger by the opt-out feature as explained above.

Extended Data Portability Scope. A controller needs to have a system for “privacy bookkeeping” in place to identify the lawful ground of processing at the point at which a portability request is received. This could, for example, be implemented in the Record of Processing.[42] As personal data that are processed based on consent are in the scope of the right to portability – and therefore the further processing of the personal data concerned is as well – controllers might want to consider granting a voluntary portability right for *all* personal data used for further processing based on compatibility too. Practically, the Record of Processing should then be extended to give insight into further processing based on compatibility. This would bring consent and compatibility to the same level for portability.

6.5 Relationship Between Compensating Measures and the Compatibility Assessment

In section 5 above we explained that it is an inherent characteristic of compatibility that shortcomings of certain factors may in some cases be compensated by better performance on other factors. Hence, the performance of the five factors can to a certain extent compensate each other. Therefore it is valuable to understand the relationship between the five capability factors (a) through (e) and the compensating measures described above.

- a. link between the purposes: *Pull notices* can be provided to increase transparency about the distance between the original and intended further purposes and about the compatibility methodology, including related policy decisions, to clarify the controller's view of the differences between the purposes. Furthermore, the controller should not leave the individual powerless and could provide *permission management* features, including *voluntary opt-out* possibilities to the individual to object to the controller's decision about the relationship between the purposes.
- b. context of data collection: *Pull notices* are a suitable means to explain the context of the intended further processing of personal data and to manage the expectations of the data subjects concerned. Another aspect is the relationship between the data subjects and the controller: in certain situations there might be a power imbalance in that relationship, for example in the employment context or where the controller has a dominant market position. The GDPR introduces a new right of data portability that empowers data subjects to get more access and control over their personal data in that it facilitates copying or transmitting personal data easily from one data controller to another. This reduces the switching barriers between controllers. *Voluntary scope extension for data portability* would enable individuals to exercise this right for all personal data used for further processing purposes.
- c. nature of data: *Pull notices* can be used to give insight into the nature of the personal data involved in the further processing, in particular whether special categories of personal data are concerned. The risk to the rights and freedoms of data subjects will differ, depending on the nature of the personal data categories involved in the processing; these might include pseudonyms or other indirect identifiers, metadata, contact details or other direct identifiers, and/or special categories of data. The controller should be transparent about the different personal data categories involved in the further processing and about its view on the potential consequences this might have for the rights and freedoms of the data subjects.
- d. possible consequences for the data subject: *Permission management* systems can enable the data subjects to manage the possible consequences for them of the intended further processing. Although the controller might do their utmost to assess these consequences for their entire data subject base, the conclusions might differ significantly from individual to individual. In practice a better approach might be to enable the data subject to make his or her own choice effectively by offering a *voluntary opt-out* option.
- e. appropriate safeguards: *Erasure trigger* connected to a *voluntary opt-out* mechanism can serve as an additional measure to ensure a level of security appropriate to the risk. Case law and the interpretation of the laws of the European data protection authorities show that controllers may be asked to observe strict – and therefore very limited – retention periods unless the controller can make a plausible case that the data has to be retained for the purposes to be achieved.[43] Moreover, additional safeguards, such as encryption or pseudonymization, might be applied to reduce the risk to the rights and freedoms of data subjects inherent to the data processed.

7 Conclusion

We have focused here on further processing of personal data that was initially collected for another purpose. The GDPR provides for further processing based on three concepts. Two of them – consent and compatibility of the future purpose with the one for which the personal data was initially collected – are the key mechanisms we researched in this article.

We assessed *whether compatibility is a useful and realistic alternative to consent in enabling further use of personal data in compliance with the GDPR* with the objective of guaranteeing a proper balance between the rights and freedoms of the data subjects concerned and the interests of the data controller, which we consider the fundamental goal of article 6(4) GDPR.

To compare these two key mechanisms, we evaluated the three most important areas of realizing privacy protection, namely (i) the privacy principles, (ii) the data subjects' rights and freedoms, and (iii) the controllers' obligations and interests.

Initially we made this comparison based on the legal bottom line of the GDPR requirements, without including any voluntary measures to improve the performance of one of the key mechanisms. We found that consent seems to be the better choice for adhering to the principles of personal data processing and to guarantee data subject rights and freedoms. In terms of feasibility of implementation, however, the compatibility mechanism appears to be the preferred solution.

By addressing shortcomings, we discussed additional measures that could achieve performance improvements that would allow compatibility to reach an equal footing with consent. All privacy principles, data subject rights, and controller obligations in which compatibility shows weaknesses have been reviewed in this respect.

Our review showed (see full overview in Appendix 1) that all shortcomings of compatibility versus consent, in almost any of the relevant factors, can be compensated for by additional measures in order to bring the compatibility mechanism to the same level as consent. The only area where compatibility cannot be elevated to an equivalent of consent is the further processing of special categories of data. Here we may continue to face limitations to finding exception grounds to lift the prohibition of further processing, as described in Appendix 1 in more detail.

Finally, we have found that the compensating measures we identified are limited in number and that permission management and active communication with the data subject are the strongest features. As many permission management systems currently available have user-centric architectures – for example, web portals, consent managers, or Customer Identity Access Management (CIAM) systems – these solutions naturally provide ideal channels for direct communication with the user. This means that these systems should potentially also be capable of providing pull notices to the data subject, thereby enabling more proactive and effective communication with the data subject, beyond the minimum required by law.

Compatibility-based processing of personal data compels the data controller to make a thorough assessment of the processing activities involved and of both the interests of the data subject and the controller, and it forces the data controller to be transparent about the processing activities that are employed.













Controllers who are prepared to implement advanced permission management systems, including features for direct communication with the data subject, may have a great potential to base many of their further processing activities on the concept of compatibility. For these advanced players in the market, consent-based further processing of personal data may become the exception rather than the rule.

Appendix 1 – Table Overview Including All Compensating Measures

The table below shows an overview of the two key mechanisms that can be applied to enable further processing of personal data. The two mechanisms of consent and compatibility are compared on the three most important aspects of realizing privacy protection: (i) the principles of personal data processing, (ii) the data subject’s rights and freedoms, and (iii) the controller’s obligations and interests.










Initially, the comparison was done with no compensating measures in place to improve the performance of one or the other of the mechanisms. In a second consideration, the compensating measures discussed above were added to improve the performance of the compatibility assessment, possibly bringing it to the same level as consent.

Table 1. Comparison of compatibility and consent as mechanisms for further processing of personal data

<i>Principles of personal data processing</i>				
<i>Privacy aspects</i>	<i>Compatibility</i>		<i>Consent</i>	
Lawfulness of processing	All lawful grounds of processing, except “Consent,” Article 6(4) jo. 6(1)(b)-(f)			All lawful grounds of processing Article 6(4) jo. 6(1)(a)-(f)
	<i>Out of scope: see assumption in section 3: Further Processing of Personal Data</i> [44]			
Transparency	Privacy notice & disclosure of standardized compatibility assessment.			Privacy notice & specific just-in-time notice per specific processing purpose.
	<i>Compensation measures:</i> • <i>pull notices</i>			
Fairness	Controller makes the decision whether new purpose is compatible with the original purpose.			Freely given consent of data subject to new purpose, while having genuine and free choice to refuse or withdraw consent without detriment.
	<i>Compensation measures:</i> • <i>pull notices</i> • <i>permission management</i> • <i>voluntary opt-out</i>			
Purpose limitation	Controller determines the remoteness of the new purpose vs. the original purpose.			Consent given by the data subject to a specific further processing purpose.
	<i>Compensation measures:</i> • <i>transparency on compatibility policy</i> • <i>permission management</i>			

	<ul style="list-style-type: none"> • <i>voluntary opt-out</i> 			
Data minimization in pursuance of proportionality and necessity principles.	Controller to determine proportionality and necessity of new purpose, while data subject has right to object if processing takes place in the context of direct marketing, public interest, or controller's legitimate interest.[45]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Data subject has the opportunity to decide if new purpose is proportional and necessary before processing starts.
	<i>Compensation measures:</i> <ul style="list-style-type: none"> • <i>permission management</i> • <i>voluntary opt-out</i> 	<input checked="" type="checkbox"/>		
Accuracy	Data subject can be educated in privacy notice on the possibilities to verify the accuracy of and rectify the personal data.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Data subject can be educated in privacy notice on the possibilities to verify the accuracy of and rectify the personal data.
Storage limitation	Controller's retention policy applies.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Controller's retention policy applies. Additionally, data subject can withdraw consent and with it trigger the erasure obligation.[46]
	<i>Compensation measures:</i> <ul style="list-style-type: none"> • <i>additional erasure trigger</i> 	<input checked="" type="checkbox"/>		
Integrity and confidentiality	Apply controller's information security baseline, including the appropriate technical or organizational measures	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Apply controller's information security baseline, including the appropriate technical or organizational measures
Accountability, i.e. demonstrate compliance with the principles above	Document compatibility assessment.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Collecting and recording of valid consent.
<i>Data Subjects – Rights and Freedoms</i>				
Subject assess request	Data subject right to get insight in personal data processed by controller is independent from lawful ground of processing.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Data subject right to get insight in personal data processed by controller is independent from lawful ground of processing.
Right to erasure	Triggered by objection to legitimate interest, but possibility to be overruled by controller.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Right to erasure triggered by withdrawal of consent.
	<i>Compensation measures:</i> <ul style="list-style-type: none"> • <i>additional erasure trigger</i> 	<input checked="" type="checkbox"/>		

	<i>ger</i>			
Right to portability	Applicable for all processing based on contract, or data provided by data subject, not otherwise.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Right to portability of consent-based processing.
	<i>Compensation measures:</i> <ul style="list-style-type: none"> <i>extended data portability</i> 	<input checked="" type="checkbox"/>		
Right to restriction	Right to restriction of processing is independent from lawful ground of processing.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Right to restriction of processing is independent from lawful ground of processing.
Right to object	Right to object if processing takes place in the context of direct marketing, public interest or controller's legitimate interest, not for other lawful grounds.[47]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Right to object triggered by withdrawal of consent in practice.
	<i>Compensation measures:</i> <ul style="list-style-type: none"> <i>unconditional opt-out option</i> 	<input checked="" type="checkbox"/>		
Choice & options	Giving choice and options to data subjects to control their data is more an objective than a legal requirement of the GDPR.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Consent giving and withdrawal mechanism is legally mandatory.
	<i>Compensation measures:</i> <ul style="list-style-type: none"> <i>permission management</i> 	<input checked="" type="checkbox"/>		
Cognitive load on the data subject	Disclosure of standardized compatibility assessment policy. Controller manages and discloses the proportionality and necessity decisions.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Risk of information fatigue of having to read multiple just-in-time notice (per specific processing purpose). Decision making is not always easy and some case not in the ability of the data subject
<i>Controller – Obligations and Interests</i>				
Controller obligations	The controller obligations (pursuant to chapter 4 of the GDPR) are independent from lawful ground of processing.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The controller obligations (pursuant to chapter 4 of the GDPR) are independent from lawful ground of processing.
International data transfer	In the presence of an adequacy decision,[48] or appropriate safeguards,[49]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	In the presence of an adequacy decision[50] or appropriate safe-

	including binding corporate rules, the obligations for international data transfer are independent from the processing ground.			guards,[51]including binding corporate rules, the obligations for international data transfer are independent from the processing ground.
Special categories of data	Limited exception grounds can be found that lift the prohibition of processing, incl. processing in the employment context, for vital or substantial public (health/research) interests, as well as for certain foundations, associations, or any other not-for-profit bodies.			Explicit consent is one of the exception grounds that lift the prohibition of processing. However, <u>explicit</u> consent requires a higher compliance standard than “ordinary” consent.
	<i>Compensation measures:</i> n/a			
Profiling, i.e. evaluating personal aspects, without making (solely automated) decision based on significance of legal effect on data subject	Under the terms of compatibility, no further approval of data subject required			Risk of low conversion rates of consent requests, as the added value of profiling might be difficult to explain to the data subject.
Implementation feasibility	Appropriate compensating measures to protect the data subject’s rights and freedoms and legitimate interests, including transparency measures might be reasonably feasible to implement.			Reaching out to the data subject might bear the risk of unsolicited communication. Collecting and recording of valid consent is challenging in practice. Providing transparent information might prove impossible or could involve a disproportionate effort.
Implementation impact	Characteristic of multifactor compatibility assessment is that shortcomings on certain factors may be compensated by a better controls on other factors.[52] This also provides the possibility to level out implementation challenges to come to a feasible mix of technical and organizational measures and controls to balance the data subject’s rights and free-			High implementation effort of technical and organizational measures and controls of collecting and recording valid consent.

	doms with legitimate interests of the controller.			
Processing continuity	Data subject has the right to object, while controller has the final say in many cases.	✓	✗	Withdrawal of consent is easy as giving it and lifts the legal ground for the processing.
Direct marketing	Unconditional right to object to direct marketing processing activities.	✓	✓	Withdrawal of consent has to be as easy as giving it.

References

- For completeness, further processing is also possible on the basis of Union or Member State law, which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) GDPR. Given the specific nature and limited scope of this feature, we will not elaborate further on this in this article.
- Report of the State Commission on the Protection of Privacy 1976, pp. 26–27.
- Blok, P.H. 2002. *Het recht op privacy* (The Right to Privacy). The Hague: Boom Juridische Uitgevers, p. 135.
- Article 5 GDPR.
- Article 6 GDPR.
- This is not a new concept: earlier, in the context of the Directive 95/46/EC, the Working Party 29 (hereinafter: WP29) published an opinion on further processing of personal data and the assessment of compatibility thereof in its working paper on purpose limitation. The GDPR codified this approach in Article 6(4).
- WP29 Guidelines on Consent under Regulation 2016/679, WP259 rev. 01, (hereinafter: WP29, WP259), adopted on 10 April 2018, p.23.
- Feiler, Lukas, Nikolaus Forgó, and Michaela Weigl. 2018. *The EU General Data Protection Regulation (GDPR): A Commentary*. Global Law and Business Ltd, UK, p.83.
- Article 4(11) GDPR and Recital 32 GDPR.
- Recital 42 GDPR.
- Recital 50 GDPR.
- Article 5(1)(b) on the principle of purpose limitation.
- Recital 50 GDPR.
- WP29, WP203, III.2.2.d, p. 26.
- Article 5(1)(b) and (e) GDPR.
- See final sentence of Article 5(1)(b) GDPR.
- WP29, WP203, p. 29.
- Pursuant to Article 5 GDPR and based on Article 8 of the European Convention on Human Rights (ECHR).
- WP29, WP259, p. 23.
- WP29 Guidelines on transparency under Regulation 2016/679, WP260 rev. 01, (hereinafter: WP29, WP260), adopted on 11 April 2018, p.20.
- WP29, WP259, p. 21.
- WP29 recognizes permission management systems as meaningful measures for “pull notices” in WP29, WP260, p.20.
- Article 21 GDPR.
- Article 17(1)(b) GDPR.
- Article 21(3) “Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.”
- It is clear from the wording of Article 21 GDPR that the balancing test is different from that found in Article 6(1)(f) GDPR. In other words, it is not sufficient for a controller to just demonstrate that an earlier legitimate interest analysis was correct. This balancing test requires the legitimate interest to be *compelling*, implying a higher threshold for overriding objections. (WP29 Guidelines on the Automated Individual Decision-Making and Profiling, WP251 rev. 01, adopted on 6 February 2018).
- Recital 7 GDPR: "Natural persons should have control of their own personal data."

28. Information Commissioner's Office (ICO). Consultation on GDPR consent guidance, March 2017.
29. Chapter 4 of the GDPR.
30. Chapter 5 of the GDPR.
31. Article 49 GDPR and WP29 Guidelines on Article 49 of Regulation 2016/679, WP262, February 6, 2018.
32. Article 9(1) GDPR.
33. Article 9(2) GDPR.
34. Articles 12, 13, and 14 GDPR.
35. WP29 Guidelines on the Automated Individual Decision-Making and Profiling, WP251 rev. 01, adopted on 6 February 2018, p. 19.
36. ICO. 2018. "Guide to the General Data Protection Regulation (GDPR)," 22 March 2018, version 1.0.34, p. 44.
37. Dutch DPA. 2015. "Wifi-tracking van mobiele apparaten in en rond winkels door Bluetrace" (Wifi-tracking of mobile devices in and around stores by means of Bluetrace), 13 October 2015 (hereinafter: Dutch DPA 2015)
38. International Association of Privacy Professionals (IAPP). 2018. "Privacy Tech Vendor Report," www.iapp.org
39. KuppingerCole. 2016. "Leadership Compass: CIAM-Platforms."
40. Gartner (2016); "Critical Capabilities for Identity and Access Management as a Service, Worldwide."
41. Ctrl-Shift. 2015. "Is the EC waking up to PIMS?" (<https://www.ctrl-shift.co.uk/news/2015/11/30/is-the-ec-waking-up-to-pims/>)
42. Article 30 GDPR.
43. Dutch DPA 2015.
44. See working assumption in section 3 that personal data initially collected based on consent will also have to be further processed based on the data subject's consent.
45. Article 21 GDPR.
46. Article 17(1)(b) GDPR.
47. Article 21 GDPR.
48. Article 45(3) GDPR.
49. Article 46 GDPR.
50. Article 45(3) GDPR.
51. Article 46 GDPR.
52. WP29, WP203, p. 22.