Lawfulness Requirements to the Storage of Customer Data in the Digital Product Passport

by **Diogo Sasdelli and Thomas J. Lampoltshammer ***

Abstract: With the advent of the Digital Product Passport (DPP), introduced in the Ecodesign for Sustainable Products Regulation (ESPR), information concerning various aspects throughout a product's value chain – from design to disposal – is to be made available in the future. This pursues the goal of promoting the establishment of a so-called circular economy in the European Union. The possibility of processing personal data within a DPP raises data protection issues, particularly concerning the lawfulness of storing customer data. Challenges arise especially in connection with the interpretation of the terms "explicit consent" and "customer" in Art. 10(1) (e) ESPR, as well as concerning the identification of the applicable sanctions in case of a violation of this article, in particular in view of the principle ne bis in idem. The paper at hand discusses these issues and proposes respective solutions.

Keywords: Digital Product Passport, Ecodesign Regulation, Data Protection, Customer Data, Explicit Consent, ne bis in idem.

Recommended citation: Diogo Sasdelli and Thomas J. Lampoltshammer, Lawfulness Requirements to the Storage of Customer Data in the Digital Product Passport, 16 (2025) JIPITEC 404 para 1.

A. Introduction

1 The central concept in the regulatory framework established by the Ecodesign for Sustainable Products Regulation (ESPR)[1] – and thus its main object – is that of the *ecodesign requirement*. Art. 2 Subpara. 1(7) ESPR defines an ecodesign requirement as "a performance requirement or an information requirement aimed at making a product, including processes taking place throughout the product's value chain, more environmentally sustainable" The ESPR thus distinguishes between two types of ecodesign requirements: (1) *performance requirements* and (2) *information requirements*. The former, according to Art. 2 Subpara. 1(8) ESPR (cf. also Art. 6 ESPR), consist of quantitative or non-quantitative requirements for or in relation to a product to achieve a certain performance level with regard to specific product parameters listed in Annex I of the ESPR. The latter, in turn, according to Art. 2 Subpara. 1(9) ESPR in conjunction with Art. 7(2) ESPR, relate to the provision of relevant information throughout the entire value chain of a product – from design to disposal. Here, the product parameters mentioned in Annex I ESPR also play a key role. These generally relate to the ecologically sustainable design of

* Diogo Sasdelli is a senior researcher at the Department for E-Governance and Administration at the University for Continuing Education Krems (Krems an der Donau, Austria); diogo.sasdelli@ donau-uni.ac.at; ORCiD: https://orcid.org/0000-0002- 6504-9812. Thomas Lampoltshammer is Professor for Information and Communication Technology and Deputy Head of the Department for E-Governance and Administration at the University for Continuing Education Krems (Krems an der Donau, Austria)thomas.lampoltshammer@donau-uni.ac.at; ORCiD: https://orcid.org/0000-0002-1122-6908.

1 Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC [2024] OJ L 1781, 28 June 2024.

products, for example with regard to repair, maintenance, and reuse possibilities, as well as their material and CO_2 footprint. The specific ecodesign requirements for respective product groups are not introduced directly by the ESPR itself, but rather by delegated acts to be adopted by the European Commission in accordance with Art. 4(1) ESPR.[2]

2 Besides the ecodesign requirements, the so-called digital product passport (DPP) also plays a prominent role in the regulatory framework of the ESPR. Its legal concept can be found in Art. 2 Subpara. 1(28) ESPR, which defines the DPP as "a set of data specific to a product that includes the information specified in the applicable delegated act adopted pursuant to Article 4 and that is accessible via electronic means through a data carrier in accordance with Chapter III."[3] In the regulatory framework of the ESPR, the DPP is directly related to the information requirements. The DPP constitutes namely the primary means by which the information requirements to be introduced in the respective delegated acts are to be fulfilled. Although the Commission may, within the framework of the respective delegated acts, grant the possibility of fulfilling information requirements by other means – e.g., through a package insert or by providing information on a website –, this should only occur in exceptional cases (e.g., according to Art. 9(4) ESPR).[4]

3 General requirements for the DPP are listed in Art. 9 and 10 ESPR and described in more detail in Annex III ESPR. These requirements stipulate, for example, that a DPP must be based on open standards (Art. 10(1)(d) ESPR) and be connected to the corresponding product via a data carrier or a unique product identifier (Art. 10(1)(a) ESPR). From a data protection perspective, however, Art. 10(1)(e) ESPR is of primary interest. It reads: "personal data relating to customers shall not be stored in the digital product passport without their explicit consent in compliance with Article 6 of Regulation (EU) 2016/679 [i.e., the GDPR[5]]". This data protection provision in the ESPR raises various questions, which can be summarised as the following three main issues:

- Personal data is generally not among the information to be provided via a DPP in order to fulfill the information requirements. It is therefore unclear under which circumstances a storage of customer data could take place. This is not a problem from a strictly legal point of view – a right may exist independently of how often it is used in practice. However, this issue can nonetheless lead to uncertainties concerning the application of the respective provisions, as further discussed below.

- The complexity of the ESPR's scope, which covers the entire value chain of numerous product groups,[6] may, under certain circumstances, lead to difficulties in defining the term "customer".

- The wording chosen by the European legislator is peculiar in that the phrase "explicit consent" does not appear in Art. 6 GDPR, which is explicitly referenced by Art. 10(1)(e) ESPR, but, e.g., in Art. 9 GDPR (i.e., in the context of so-called *sensitive* data), thus leading to unclarity concerning the kind of consent required by Art. 10(1)(e) ESPR.

4 In the following, to adequately contextualise these three issues, Section B first provides an overview of the main technical elements of a DPP. Then, these issues are discussed in more detail in Section C. A further problem involves determining the applicable sanctions in case of violations of Art. 10(1)(e) ESPR, i.e., whether GDPR-sanctions, ESPR-sanctions or potentially both should be applicable. This matter is discussed below in Section D. Section E concludes.

B. Digital Product Passport – Technical Overview

5 From a technical point of view, a DPP can be

2 In its normative function, the ESPR is thus primarily to be regarded as an authorisation norm (Ermächtigung). Cf eg Hans Kelsen, *Allgemeine Theorie der Normen* (Manz 1979) 82–84; Hans Kelsen, *Reine Rechtslehre* (2nd edn, Mohr Siebeck 2017) 114–16. For this reason, the clarification of most questions surrounding the DPP is left to tertiary law; cf Florian Fuchs-Zeitner, 'Der Digitale Produktpass (DPP) nach der neuen ÖkodesignVO – Klarheit erst durch geplantes Tertiärrecht' [2024] ZUR 534.

3 For a discussion of the problems associated with this definition, see Diogo Sasdelli and Verena Schmid, 'Legal Challenges and Technical Solutions to Decentralised Digital Product Passports' in Ulrike Lucke and others (eds), *INFORMATIK 2025*(Gesellschaft für Informatik 2025) 53. For a detailed discussion of the DPP concept beyond its purely legal framework, see eg Adrian Barwasser and others, *Der Digitale Produktpass* (Fraunhofer-Institut für Arbeitswirtschaft und Organisation 2024).

4 Cf Diogo Sasdelli and Verena Schmid, 'Legal Challenges and Technical Solutions to Decentralised Digital Product Passports' in Ulrike Lucke and others (eds), *INFORMATIK 2025* (Gesellschaft für Informatik 2025) 53, 62.

5 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 (General Data Protection Regulation) [2016] OJ L119/1.

6 Cf Anne-Christin Mittwoch, 'Der digitale Produktpass der Ökodesign-Verordnung. Passierschein zur erfolgreichen Zwillingstransformation im produktrecht?' [2024] Recht Digital 62.

conceptualised as a representation of a digital record, comprising detailed information concerning a particular product, spanning its entire lifecycle.[7] It is designed to enable informed decision-making throughout product lifecycles, hence also contributing to the circular economy.[8] Against this backdrop, the DPP can be understood as a transformation enabler beyond mere regulatory compliance.[9] To use an analogy, a DPP can be considered as an equivalent of a so-called *digital twin* of the corresponding physical product,[10] with its specified underlying data structure defined through frameworks such as the Asset Administration Shell (AAS). The AAS provides a standardised metamodel, which enables consistent description, management, and exchange of information concerning assets throughout their lifecycle.[11]

6 One possibility for the unification and effective management of the inherently heterogeneous data across different value chains in regard to the DPP system comes via the use of so-called ontologies and knowledge graphs (KGs).[12] A simplified DPP model[13] can be understood through the following interconnected elements:

- The DPP (i.e., the digital twin of the product);
- A persistent unique product identifier (UID), which is bi-uniquely linked to both the product and the DPP and establishes a connection (or linking) between the product and the DPP (or the data storage in which the DPP is stored);
- A decentralised data storage in which the DPP is stored;
- A data carrier that is physically linked to the product and can be read to call up the DPP using the persistent unique product identifier.

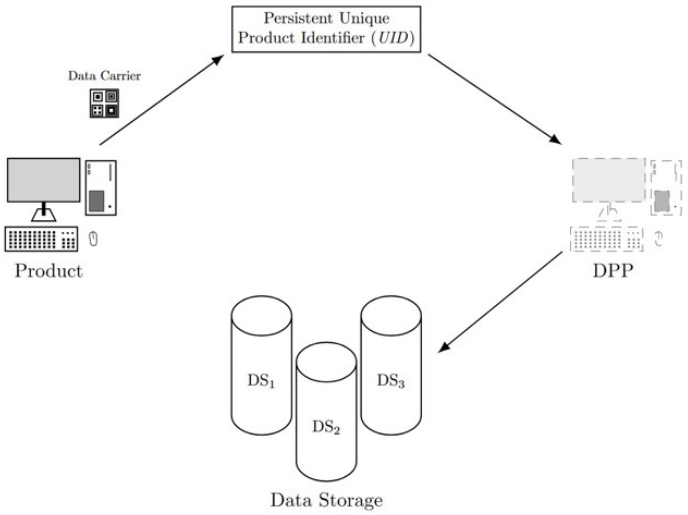

Fig.1. Simplified DPP Model

This simplified DPP model can be visualised in Fig. 1 (above):

7 Cf Monireh Pourjafarian and others, 'A Multi-Stakeholder Digital Product Passport Based on the Asset Administration Shell' in *IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)* (IEEE 2023) 1.

8 Cf Steffen Foldager Jensen and others, 'Digital Product Passports for a Circular Economy: Data Needs for Product Life Cycle Decision-Making' [2023] *Sustainable Production and Consumption* 242.

9 Cf Arko Steinwender and others, 'From Analogue to Digital Product Passports in the Furniture Industry' [2024] *IFAC-PapersOnLine* 229.

10 Cf Joerg Walden, Angelika Steinbrecher and Maroye Marinkovic, 'Digital Product Passports as Enabler of the Circular Economy' [2021] *Chemie Ingenieur Technik* 1717; Anne-Christin Mittwoch, 'Der digitale Produktpass der Ökodesign-Verordnung. Passierschein zur erfolgreichen Zwillingstransformation im produktrecht?' [2024] *Recht Digital* 62.

11 Cf Monireh Pourjafarian and others, 'A multi-stakeholder digital product passport based on the asset administration shell' in *IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)* (IEEE 2023) 1, 2.

12 Cf Anastasiia Belova and others, 'Bringing the Digital Product Passport to Life: Requirements Analysis for a Carbon Footprint Tracking System Using Knowledge Graphs and Data Spaces' in *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing* (ACM 2025) 490, 493.

13 This model is strongly simplified. It sets aside, e.g., the complex data-space related architectures and exchanges required to enable the creation, modification and the reading of DPPs by different stakeholders.

C. Legality of Storing Customer Data in the Digital Product Passport

I. Personal Data and Customer Data in the Digital Product Passport

7 First, it seems appropriate to clarify under which circumstances one should expect the processing of personal data and, in particular, the storage of customer data in a DPP. According to Art. 7 ESPR, one would expect that the information requirements to be issued by the Commission will generally concern information about the product's performance in relation to parameters mentioned in Annex I ESPR, as well as information on the handling of the product throughout its entire life cycle (e.g., installation, maintenance, repair, disposal, etc.). Obviously, this kind of information does not normally constitute personal data. Only a more detailed analysis of the specific requirements set for DPPs reveals scenarios in which the processing of personal data might take place: Art. 9(2)(a) ESPR in conjunction with Annex III ESPR provides that the Commission may determine, in the respective delegated acts, that certain data be included in the DPP. Along these are, for example, information concerning the manufacturer (Annex III(1)(g) ESPR) and other so-called *economic operators* (Annex III(1)(h-k) ESPR), as well as so-called *digital product passport service providers* (Annex III(1)(l) ESPR). According to Art. 2 Subpara. 1(46) ESPR, an *economic operator* is defined as a *manufacturer*, an *authorised representative*, an *importer*, a *distributor*, a *dealer*, or a *fulfillment service provider*. All these actors can, according to the given definitions (cf. Art. 2 Subpara. 1(42), (43), (44), (45), (55) ESPR and Art. 2 Subpara. 10 ESPR in conjunction with Art. 3(11) of the Regulation (EU) 2019/1020), be natural persons, which would generally establish the data protection relevance of corresponding data processing. However, these actors are generally not to be understood as customers. This can be derived from the fact that the ESPR also contains a definition of "customer", which is excluded from the list in the aforementioned definition of "economic operator". Through a similar line of thought, it can be argued that, although digital product passport service providers may be natural persons, they are generally not to be considered as being customers.[14]

8 Beyond these passages, the ESPR provides almost no further relevant insights on the circumstances under which one would expect the processing of personal data, in particular of customer data, within a DPP. Among its enacting terms, data protection-relevant processing is only mentioned in Art. 10(1)(e) ESPR (i.e., the prohibition of storing customer data without their explicit consent) as well as in Art. 13(1)(4) ESPR and Art. 13(3) ESPR, which, however, do not refer to data processing within the DPP itself, but to data processing in connection with the administration of the DPP registry to be established according to Art. 13 ESPR. The recitals also contain no further relevant information. The relevant Recital 43 merely states that the processing of personal data within the framework of the ESPR must comply with applicable data protection rules (in particular the GDPR). Particularly striking is the fact that the last sentence of Recital 43 ESPR clearly contradicts Art. 10(1)(e) ESPR by stating: "Personal data of customers should not be stored in the digital product passport."

9 Analysing the documentation on the legislative process reveals an interesting development. In the original proposal from 2022, data protection-relevant processing was only mentioned in connection with the DPP registry – at that time in Art. 12(1)(3) and Art. 12(3), which basically correspond to Art. 13(1)(4) and Art. 13(3) of the final version of the ESPR.[15] In particular, the original proposal lacked the last sentence in the then Recital 35 (in the final version Recital 43 ESPR), according to which customer data should not be stored in the DPP. It is only with the amendments adopted by the European Parliament on 12.07.2023 that first developments towards the final wording can be identified. The then Recital 35 (now Recital 43) was supplemented by the sentence "Personal data of end-users should not be stored in the digital product passport." Accordingly, a *littera* "da" was added to Art. 9(1)(1) with the content: "personal data relating to the end-user of the product may not be stored in the product passport".[16]

14 In this respect, the German version of the ESPR has an interesting particularity: it employs two different wordings for the DPP service provider. It initially uses the wording 'Digitalproduktpass-Dienstleister' (eg in recitals 38 and 40 and in art 2 subpara 1(32) ESPR). From art 10(4) ESPR onwards, with the exception of art 11(3) ESPR, the term used is always 'unabhängiger Digitalproduktpass-Drittdienstleister'. Since this is a peculiarity of the German version, it seems reasonable to assume that this terminological inconsistency is due to clumsy drafting or even an error. These German wordings should therefore be considered synonyms, so that the definition of 'Digitalproduktpass-Dienstleister' given in art 2 subpara 1(32) ESPR should also be directly applicable to the term 'unabhängiger Digitalproduktpass-Drittdienstleister'.

15 Cf European Commission, 'Proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC' COM(2022) 142 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0142 accessed 12 November 2025.

16 Cf European Parliament, 'Amendments adopted by the European Parliament on 12 July 2023 on the proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements

The final version, in which "end-user" was replaced by "customer" in these passages, can be recognised at least since the version of 22.12.2023, which was formulated after the informal negotiations in the *trilogue* procedure.[17] Although the final version of the ESPR contains both the term "customer" and the term "end-user", the data protection provisions always refer to "customer". This development points to a conscious decision by the European legislator with regard to the data protection provisions in favour of using the term "customer" – as defined in Art. 2 Subpara. 1(35) ESPR – instead of the term "end-user" – as defined in Art. 3(21) of Regulation (EU) 2019/1020. The specific consequences of this decision for the requirements for the storage of customer data will be discussed in more detail below.

II. Definition of Customer Data

10 The provision in Art. 10(1)(e) ESPR states: "Personal data relating to customers shall not be stored in the digital product passport without their explicit consent in compliance with Article 6 of Regulation (EU) 2016/679 [i.e., the GDPR]". Thus, the term "customer data" contains two basic elements; in other words: "customer data" is (1) *personal data* that (2) relate to *customers*.

11 Although not explicitly prescribed in the ESPR, it is reasonable to assume that the definition of *personal data* given in Art. 4(1) GDPR is to be adopted here. Accordingly, personal data is "any information relating to an identified or identifiable natural person [...]". The rest of Art. 4(1) GDPR contains provisions on the circumstances under which a natural person is to be considered identified or identifiable.[18]

12 The relevant concept of customer is given in Art. 2 Subpara. 1(35) ESPR. Accordingly, a *customer* is "a natural or legal person that purchases, hires or receives a product for their own use whether or not acting for purposes which are outside their trade, business, craft or profession". As mentioned above, the European legislator has deliberately opted for using the term "customer" instead of the term "end-user" in matters pertaining to the protection of personal data. The definition of the latter term can be found, according to Art. 2 Subpara. 10 ESPR, in Art. 3(21) of the Regulation (EU) 2019/1020. Accordingly, an "end user" is "any natural or legal person residing or established in the Union, to whom a product has been made available either as a consumer outside of any trade, business, craft or profession or as a professional end user in the course of its industrial or professional activities". These terms are generally quite similar: both refer to natural *or* legal persons; both allow for commercial or business purposes, but also for private, non-commercial purposes. However, these terms differ in two main aspects:

- Only the *end-user* must have a residence or establishment in the Union. For the *customer*, no requirements regarding their residence are specified.

- To meet the definition of a customer, the product must be bought, leased, or received *for own use*. In contrast, for the "end-user", it is sufficient to be the person to whom the product has been *made available*. "Making available *on the market*" means, according to Art. 2 Subpara. 1(39) ESPR – or to the *ipsis litteris* identical Art. 3(1) of Regulation (EU) 2019/1020 – "any supply of a product for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge". The crucial difference between the two definitions is that in the case of the customer concept, due to the phrase "for own use", the form of acquisition (purchasing, hiring, receiving) is directly linked to the actor (the customer). The term "end-user" (in this definition, "end user" is written without hyphenation), on the other hand, allows for acquisition and use to be carried out by different actors. A *customer* is therefore an *end-user* with any residence or establishment who also carries out the acquisition of the corresponding product themselves (i.e., buys, hires, or receives it).[19]

13 This distinction has the direct consequence that the special protection introduced in Art. 10(1)(e) ESPR – i.e., the requirement of *explicit consent* for lawful storage in a DPP – will not apply to data subjects who do not acquire the respective product for their own use and are therefore not customers in the sense of Art. 2 Subpara. 1(35) ESPR. This would be the case, for example, if someone buys an electronic device as a

for sustainable products and repealing Directive 2009/125/EC' P9_TA(2023)0272 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023AP0272> accessed 12 November 2025.

17 Cf Council of the European Union, 'Regulation establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC – Letter to the Chair of the European Parliament ENVI Committee' ST 5147/2024 INIT <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL:ST_5147_2024_INIT> accessed 12 November 2025.

18 For more details on identifiability, see eg Andreas Bergauer in Hubert Jahnel (ed), *DSGVO* (2020) art 4 para 14–16.

19 In cases in which someone merely receives a product free of charge, there would be no meaningful difference between a customer and an end-user (beyond the requirement concerning residence or establishment). For *receiving*, according to common usage, is, unlike *buying* or *hiring*, a *passive* activity: whoever receives something is at the same time always the person to whom this thing is made available.

gift for a friend. The lawfulness of the storage of her data in a DPP would follow not Art. 10(1)(e) ESPR, but the usual data protection provisions – in particular Art. 6(1) GDPR. Since, however, neither the payment nor the source of the acquisition is relevant for satisfying the definition of "customer", the friend would, in this case, certainly be considered as being a customer, being thus entitled to the special protection of Art. 10(1)(e) ESPR.

14 The protection status of data subjects who have a dual nature, i.e., subjects who could be considered as customers in the sense described above while, at the same time, being potentially also subsumable under another category, constitutes a difficult question. This can occur *synchronously* – i.e., the person is simultaneously a customer and something else – or *asynchronously* – i.e., the person *becomes* a customer. Such scenarios can arise when the data subject acts as an *economic operator* or as a *DPP service provider* – so that personal data concerning them (as discussed above in section 2.1) may, under certain circumstances, have to be stored in the DPP according to the respective delegated acts – and they are simultaneously a customer or become a customer at a later date.[20]

15 In such cases (i.e., if the data subject assumes both the role of the customer and another role in the DPP architecture, e.g., as an economic operator), following the literal wording of the legal provisions and assuming no explicit consent was given by the data subject, the storage of data in a DPP would generally *not* constitute an unlawful processing in the sense of the GDPR – especially since Art. 6(1)(c) GDPR would likely be applicable. However, such a scenario would indeed violate Art. 10(1)(e) ESPR, which prohibits the storage of customer data in the absence of explicit consent. This result is problematic for two reasons. First, it seems to impose an unreasonable obligation of the respective controller – or DPP operator – to permanently check the customer status of any data subjects. Second, it leads to the fact that the realistic implementation of Art. 10(1)(e) ESPR would be tantamount to prescribing that any storage of personal data in a DPP require explicit consent, since *eo ipso* every person is always a potential customer. This, however, would contradict the explicit restriction of Art. 10(1)(e) ESPR as a special protection given only to personal data of *customers*.

16 Thus, it seems more appropriate to always evaluate the *customer status* in connection with the context underlying the data storage in the DPP: for the purposes of Art. 10(1)(e) ESPR, the storage of customer data in the DPP *sensu proprio* does not concern the mere storage of any personal data concerning customers, but rather the storage of such data *on the basis of* (or at least in direct connection with) the customer status of the respective data subjects. Against the objection that this solution would represent an interpretation that restricts the fundamental right to data protection compared to the literal interpretation outlined above, one could argue that the provisions of the GDPR – which are still applicable anyway –, guarantee a perfectly adequate level of protection, so that the restriction involved in the interpretation proposed here is based on a justifiable balancing of interests, especially in view of the aforementioned unreasonable consequences of the literal interpretation.

III. Explicit Consent

17 According to Art. 10(1)(e) ESPR, customer data may not be stored in the DPP without their "explicit consent" in compliance with Art. 6 GDPR. This wording is problematic because on the one hand it seems to require a qualified form of consent, namely *explicit* consent, but on the other hand it refers to Art. 6 GDPR, which, however, does not speak of *explicit* but merely of a not further specified, hence simple consent. It is therefore unclear whether simple consent in the sense of Art. 4(11) GDPR is sufficient to fulfil Art. 10(1)(e) ESPR or whether a qualified form of consent is required.

18 The term "consent" is defined in Art. 4(11) GDPR. Accordingly, "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". However, the GDPR contains no explicit definition of a qualified, *explicit* consent. This raises the question of the difference between mere consent on the one hand and a qualified, *explicit* consent on the other, which shall be discussed in the subsection at hand incidentally.

19 As already mentioned above, the definition in Art. 4(11) GDPR contains no provisions regarding a qualified, explicit consent. Similarly, Art. 6(1)(a) GDPR (and the corresponding Recital 32) only mention (simple) "consent", without any further qualifications. According to Art. 6(1)(a) GDPR, processing is only lawful if the data subject has given their (simple) consent. The phrase "explicit consent" first appears in Art. 9(2)(a) GDPR, i.e., the counterpart to Art. 6(1)(a) GDPR in the more specific case of processing of special categories of personal data. Accordingly, this more sensitive kind of data may only be processed if the data subject has *explicitly*

20 Another conceivable scenario would concern the storage of data concerning persons who, for example, as engineers are responsible for the safety of chemical or technical products.

consented to the data processing. Furthermore, an "explicit consent" is also required in the context of protection against automated individual decision-making, including profiling (Art. 22(2)(c) GDPR), and for data transfers to third countries or international organisations (Art. 49(1)(a)). The corresponding Recitals 51, 71, and 111 also use the phrase "explicit consent". All this suggests the interpretation that the European legislator has introduced not only the notion of a simple consent but also a qualified, explicit form of consent, which is to be regarded as an additional requirement in particularly sensitive cases.[21]

20 While this would *prima facie* justify the existence of "explicit consent" as a legal concept within the framework of the GDPR, the regulation still offers no adequate information to determine the content of this concept, i.e., the specific additional requirements associated with it. The European Data Protection Board (EDPB) adopts the view that *explicitness* refers to the way in which the data subject expresses their consent.[22] The EDPB attempts to clarify this rather vague explanation with examples: As an "obvious way to make sure consent is explicit", the EDPB gives the example of consent that is "expressly [confirmed] in a written statement".[23] This *explicit confirmation* could be achieved by the data subject signing the written statement in which the consent had been given.[24] In this sense, an *explicit consent* would be understood as a (simple) consent that is explicitly confirmed – for example, by a signature of the data subject. The EDPB thus seems to suggest a *two-step procedure* for an explicit consent: the (still simple) consent would first have to be given and then confirmed, thereby making it an explicit consent. This interpretation also seems to underlie other examples given by the EDPB:

- When obtaining consent via e-mail, the controller can, after receiving the consent, send a confirmation link or an SMS message with a confirmation code to the data subject, through which the consent is confirmed.[25]

- When obtaining oral consent in a telephone conversation, the data subject can confirm their given consent by pressing a button or also orally.[26]

21 However, the EDPB seems to abandon this two-step structure in other examples it provides. It claims, for instance, that a controller can obtain explicit consent from visitors to its website via a standard cookie banner, as long as the consent is clearly shown in the text – e.g., with the wording "I, hereby, consent to the processing of my data", but not with the wording "It is clear to me that my data will be processed".[27] This, however, blurs the line between simple and explicit consent.

22 In general, the legal-dogmatic clarification of this problem is not yet mature. The topic is relatively ignored in the literature; in most cases, reference is simply made to the not very enlightening statement of the EDPB, with some aspects concerning the explicitness of consent being emphasised. Some, for example, point out that explicit consent is characterised by an explicit reference to the respective nature of the data that will be processed.[28] Others emphasise that merely *implied* consent does not meet the requirement of explicitness.[29] Aspects

21 Cf eg Council of the European Union, 'Draft Statement of the Council's Reasons concerning the Position of the Council at First Reading with a View to the Adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and repealing Directive 95/46/EC' ST 5419/2016 ADD 1 REV 1 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_ADD_1_REV_1> accessed 12 November 2025, 9, where explicit consent is described as a 'higher threshold'. Cf also Christopher Schulz in Peter Gola and Benedikt Heckmann (eds), *DSGVO* (3rd edn 2022) art 9 para 23.

22 EDPB, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (2020) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de> accessed 12 November 2025, para. 93.

23 Ibid.

24 Ibid.

25 European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (2020) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de> accessed 12 November 2025, para 98.

26 European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (2020) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de> accessed 12 November 2025, para 95.

27 European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (2020) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de> accessed 12 November 2025, para 96.

28 Christopher Schulz in Peter Gola and Benedikt Heckmann (eds), *DSGVO* (3rd edn 2022) para 23; Thilo Weichert in Jürgen Kühling and Benedikt Buchner (eds), *DSGVO* (1st edn 2017) art 9 para 47; Benedikt Buchner in Jürgen Kühling and Benedikt Buchner (eds), *DSGVO* (1st edn 2017) art 22 para 42.

29 Jens Ambrock and Moritz Karg, 'Ausnahmetatbestände der DS-GVO als Rettungsanker des internationalen Datenverkehrs?' [2017] *ZD* 154, 157; Hubert Jahnel in Hubert Jahnel (ed), *DSGVO* (2020) art 9 para 52; Peter Kastelitz,

such as the data subject's capacity of discernment and the associated voluntariness of the consent are also mentioned.[30]

23 However, these observations still do not provide a satisfactory basis for distinguishing *explicit* from merely *simple* consent, because all the aspects emphasised above can – at least in a weaker form – also be considered as requirements for simple consent in the sense of Art. 4(11) GDPR. The demand for an explicit reference to nature of the data to be processed can, for example, be derived on the one hand from the definition in Art. 4(11) GDPR, which links the consent to the respective specific case, and on the other hand from the purpose limitation principle (Art. 5(1)(b) GDPR). The capacity of discernment and voluntariness of the consenting subject, in their turn, result directly from Art. 4(11) GDPR. The exclusion of implied consent from the scope of explicit consent, which is almost universally represented in the literature, also proves to be unjustified upon closer examination. The concept of *implied consent* is constructed directly on the basis of the definition in Art. 4(11) GDPR, according to which consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". An "implied consent" would therefore be understood as any consent that is not given by a statement, but by a *clear affirmative action*.[31] In this sense, the scope of the term "explicit consent" would consist either in the corresponding complementary set to the scope of "implied consent" or in a proper subset thereof. In other words: explicit consent would be all and only those types of consent that are given in the form of (possibly further qualified) *statements*.

24 Despite its elegance, this conceptual construction must be rejected. In general, it seems inappropriate to exclude, as a matter of principle, *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her* from being an explicit consent.

25 In addition, some of the examples of explicit consent cited by the EDPB – such as pressing buttons or accessing links – can certainly be considered as type of *implied* consent, i.e., consent based on affirmative actions instead of on statements.[32] *Last but not least*, the exclusion of implied consent from the scope of explicit consent would be inconsistent with the case law of the ECJ, which, when considering a case in which a person had manifestly made public information about their sexuality in a panel discussion open to the public, considered that this does not allow the conclusion that the person had given their "consent within the meaning of Article 9(2)(a) of the GDPR to processing of other data relating to his or her sexual orientation by the operator of an online social network platform".[33] If it were true that an implied consent, as a matter of principle, could not constitute an explicit consent, the ECJ would only need to point this out, instead of examining the suitability of the action as consent to a specific processing. The fact that the ECJ examined the matter means, by way of *e contrario* reasoning, that implied consent can, under certain circumstances, also meet the requirements for explicit consent.[34]

Helmut Hötzendorfer and Christoph Tschohl in Nikolaus Knyrim (ed), *DSGVO* (2020) art 9 para 31; Christopher Schulz in Peter Gola and Benedikt Heckmann (eds), *DSGVO* (3rd edn 2022) art 9 para 23; Daniel Pauly in Boris Paal and Daniel Pauly (eds), *DSGVO* (3rd edn 2021) art 49 para 7; Arne Klement in Spiros Simitis, Gerrit Hornung and Indra Spiecker genannt Döhmann (eds), *DSGVO* (2025) art 7 para 28; Jonathan Petri in Spiros Simitis, Gerrit Hornung and Indra Spiecker genannt Döhmann (eds), *DSGVO* (2025) art 9 para 33.

30 Cf Mario Martini in Boris Paal and Daniel Pauly (eds), *DSGVO* (3rd edn 2021) art 22 para 38; Daniela Alaattinoğlu, 'Rethinking Explicit Consent and Intimate Data: The Case of Menstruapps' [2022] *Feminist Legal Studies* 157.

31 Stefan Stemmer in Heinrich Wolff, Christoph Brink and Carl von Ungern-Sternberg (eds), *DSGVO* (52nd edn 2025) art 7 para 84; Arne Klement in Spiros Simitis, Gerrit Hornung and Indra Spiecker genannt Döhmann (eds), *DSGVO* (2025) art 7 para 28.

32 In a slightly weaker form, the distinction between implied and explicit consent is based on the argument that the latter requires at least an 'affirmative gesture' (bejahende Geste). Cf, for example, Jens Ambrock and Moritz Karg, 'Ausnahmetatbestände der DS-GVO als Rettungsanker des internationalen Datenverkehrs?' [2017] *ZD* 154; Towfigh and Ulrich in Nils-Christian Sydow (ed), *DSGVO* (2nd edn 2018) art 49 para 5, who, however, with the extremely unfortunate wording 'Ausdrücklich ist die Einwilligung, wenn sie nicht konkludent erfolgt ist, mithin auf einer bejahenden Geste beruht' (ie, consent is explicit when it is not given implicitly, but is based on an affirmative gesture) get somewhat tangled in their words, as this would literally mean that only consent based on gestures could be explicit, which is, of course, nonsensical. In general, the inclusion of gestures in the scope of explicit consent leads to a blurring of the distinction between explicit and implied consent. Cf also Benedikt Buchner and Jürgen Kühling in Jürgen Kühling and Benedikt Buchner (eds), *DSGVO* (4th edn 2024) art 7 para 58b.

33 Cf Case C-446/21 Maximilian Schrems v Meta Platforms Ireland Ltd EU:C:2024:834, para 82.

34 Against this would prima facie speak Case T-343/13 *XYZ v European Data Protection Supervisor* (EGC, 3 December 2015) para 62, which states that explicit consent is not satisfied

26 Some clarity in this otherwise quite challenging conceptual construction can be found, assuming a change of perspective, precisely in Art. 10(1)(e) ESPR, which was initially seen as the root of the problem. Its supposed problem is that, on the one hand, according to it, the storage of customer data in the DPP requires *explicit consent*, while on the other hand, it explicitly refers to Art. 6 GDPR, which, however, only requires an unspecified or simple, not an explicit consent, which appears contradictory. This problem, however, is based on the assumption that the data protection framework established by the GDPR actually recognises two types of consent, i.e., that it distinguishes between explicit and non-explicit (e.g., implied) consent. If this assumption is abandoned, the problem disappears. Indeed, a harmonious interpretation of Art. 10(1)(e) ESPR in conjunction with Art. 6(1)(a) GDPR, which preserves the fundamental coherence of the European legislator, suggests, rather, that there is in fact only one form of consent, or that the *explicitness* of an explicit consent does not refer to a special category or form of consent, but to *something else*.

27 All four cases in which explicit consent is required – particularly sensitive data (Art. 9(2)(a) GDPR), automated decisions (Art. 22(2)(c) GDPR), data transfers to third countries (Art. 49(1)(a) GDPR), and now also the storage of customer data in the DPP (Art. 10(1)(e) ESPR) – can be considered as situations requiring a particularly high degree of protection. From this realisation, it can be concluded that the explicitness of consent is intended to grant special protection against unlawful processing, which, in turn, serves the purpose of protecting against a violation of the underlying fundamental right to the protection of personal data, the explicitness of an explicit consent cannot therefore refer to exclusively allowing a special, qualified form of consent. Instead, it must refer to ensuring that consent was *actually* – or rather, *factually* – given. Explicitness of consent refers therefore not to additional requirements for the already demanding definition of consent in the sense of Art. 4(11) GDPR (cf. also the requirements in Art. 7 GDPR), but to additional requirements concerning the *proof* that consent has actually been given for the respective processing. Explicitness is therefore not to be regarded as a realisation of the principle of lawfulness (Art. 5(1)(a) GDPR), but as a realisation of the principle of accountability (Art. 5(2) GDPR). It means specifically that, whenever explicit consent is required, one must proceed carefully and always demand high standards when assessing the evidence of consent provided by the controller.

28 Concluding, one can therefore assume that, in practice, the proof of a merely *implied* consent will generally not succeed under the additional requirements arising from explicitness. At the same time, however, it will not be possible to exclude *a priori* that an implied consent could, under certain circumstances, nevertheless meet these requirements.[36] The same applies with regard to Art. 10(1)(e) ESPR for the storage of customer data in the DPP.

D. Sanctions

29 Finally, the question must be addressed as to which sanctions can be imposed in the event of a violation of Art. 10(1)(e) ESPR. It is important to distinguish between two scenarios, i.e., whether (1) the action leading to a violation of Art. 10(1)(e) ESPR simultaneously also constitutes a violation of the GDPR (e.g., of Art. 6 GDPR, or possibly also of Art. 9 GDPR) or (2) Art. 10(1)(e) ESPR is violated without also incurring in a violation of the GDPR.

if consent is 'implicitly derived from the actions of the data subject'. However, this statement does not concern the notion of 'explicit consent' under the GDPR, but rather art 10(2)(a) of Regulation (EC) 45/2001. The relevant definition was therefore that in art 2(h): '"the data subject's consent" shall mean any freely given specific and informed indication of his wishes, signifying his agreement to personal data relating to him being processed'. Unlike the corresponding definition in the GDPR, this definition contains no explicit indication that implied consent may be sufficient; it is therefore a priori much narrower.

35 Cf eg art 8(2) CFR, which refers only to 'consent'.

36 This view is apparently also adopted by Thilo Weichert in Jürgen Kühling and Benedikt Buchner (eds), *DSGVO* (1st edn 2017) art 9 para 47, who argues that, with regard to explicit consent, conclusive action is largely excluded ('schlüssiges Handeln weitgehend ausgeschlossen ist'). Likewise, Peter Schantz in Spiros Simitis, Gerrit Hornung and Indra Spiecker genannt Döhmann (eds), *DSGVO* (2025) art 49 para 12, appears to lean towards this view by arguing—in a way coherent with as a continuation of the legal situation under art 26(1)(a) of the Data Protection Directive (Directive 95/46), which was replaced by the GDPR—that, for the lawfulness of data transfers to third countries, it is necessary that the data subject gives consent without any doubt ('die betroffene Person ohne jeden Zweifel ihre Einwilligung [abgibt]').

30 A violation of Art. 10(1)(e) ESPR, for example, is generally *not* accompanied by a violation of the GDPR if customer data is processed without (explicit) consent, but on the basis of another legally relevant reason under Art. 6 GDPR. It is also possible to conceive of situations in which the storage of customer data occurs outside the scope of the GDPR (Art. 2 and 3 GDPR). This could be the case, for example, if a manufacturer (in this case generally also the controller in the sense of Art. 4(7) GDPR) without an establishment in the Union stores data of customers in the DPP who have not given their consent and are not located in the Union, but the corresponding products, together with the DPP, are introduced into the internal market by the importer. In such cases, only the ESPR is violated, so that any sanctions are to be imposed according to the standards set out in Art. 74 ESPR.

31 According to Art. 74(1) ESPR, Member States must lay down rules on sanctions applicable to infringements of the ESPR. These sanctions must also be effective, proportionate, and dissuasive. According to Art. 74(2) ESPR, several aspects are to be taken into account, such as the nature, gravity, and duration of the infringement, the financial situation of the natural or legal person held responsible, whether the infringement was repeated or a one-off event, among other factors. Finally, Art. 74(3) ESPR provides that Member States may impose at least fines or a temporary exclusion from public procurement as sanctions.

32 Compared to the GDPR, which in its Art. 83 sets precise upper limits for fines for infringements of certain provisions, the ESPR contains only relatively vague provisions on applicable sanctions. Here, it seems reasonable to take the sanctions listed in the respective implementation laws for the older Ecodesign Directive (2009/125/EC), which has now been replaced by the ESPR, as a reference value. Comparing different Member States, however, leads to a rather colourful picture: In Germany, for example, according to § 13 of the Act on the Ecodesign of Energy-related Products (*Gesetz über die umweltgerechte Gestaltung energieverbrauchsrelevanter Produkte –EVPG*), fines of up to €10,000, in some cases even up to €50,000, can be imposed. The Portuguese *Decreto-lei n.° 12/2011* is at a similar level, with its Art. 16 providing for fines from €3,000 to €44,750. The sanctions are somewhat stricter in Italy, which, according to Art. 17 of the *Decreto Legislativo 16.02.2011, n. 15*, can reach a height of up to €150,000 in the most serious cases. Sky-high fines can be imposed in Spain: The Spanish *Real Decreto 187/2011* refers for sanctions to the provisions of the *Ley 21/1992*, according to whose Art. 34 fines of up to 100 million euros are possible for very serious (*muy grave*)[37] cases. In a rather striking contrast, the Austrian Ecodesign Ordinance (*Ökodesign-Verordnung* – ÖDV 2007) provides for *no* fines at all. According to § 7(1) ÖDV 2007, the market surveillance authority, in case of sufficient indications of an infringement, *shall take the necessary measures, which may range from prohibiting the placing on the market of the product concerned [...] depending on the severity of the infringement.*

33 In the absence of more specific provisions concerning sanctions, this regulatory dissonance is likely to persist in the new legal framework introduced by the ESPR. The applicable sanction is therefore likely to vary greatly depending on the Member State. This is particularly problematic when – as is to be expected with violations of Art. 10(1)(e) ESPR – the respective violation is, *ceteris paribus*, felt cross-border, and thus a parallel initiation of corresponding fine proceedings in several Member States seems likely. This leads to the question of the possibility of *double jeopardy*, which also arises in the context of violations of Art. 10(1)(e) that simultaneously also constitute a violation of the GDPR – e.g., the storage of customer data in the DPP without any legal basis. Specifically, it must be examined here whether double jeopardy in such cases is compatible with the principle of *ne bis in idem* or not.

34 The principle of *ne bis in idem* is a classic principle of criminal procedure law and, as such, is codified in several national and international legal systems – often with the character of a fundamental right. In European law, the principle is enshrined in Art. 50 CFR, in Art. 4 of Protocol 7 to the ECHR, and in Art. 54 of the Schengen Implementing Convention. In Art. 50 CFR, the principle is described as the right "not to be tried or punished twice in criminal proceedings for the same criminal offence". Specifically, the provision reads: "No one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law" The terms "criminal", "criminal offence", and "criminal proceedings" are to be interpreted rather broadly – also due to the fundamental rights character of the principle. Thus, fines imposed by authorities according to administrative law provisions or corresponding proceedings also fall under Art. 50 CFR, as long as they have a high degree of severity and a repressive objective is pursued with them.[38] Furthermore, the

37 According to art 31(1)(a) of Real Decreto 187/2011, very serious infringements include, among others, the intentional violation of relevant provisions where this results in a high risk to, or damage for, individuals. Given the data-protection character of art 10(1)(e) ESPR, it does not seem implausible that violations of this provision could also be classified as very serious.

38 Cf eg Case C-27/22 *AGCM v Ryanair DAC* EU:C:2023:663, headnote 1; Case C-857/19 *DB v Commissione nazionale per*

principle protects not only natural persons, but also companies or legal persons from double jeopardy.[39] Thus, the applicability of the principle of *ne bis in idem* against double jeopardy for violations of Art. 10(1)(e) ESPR is *prima facie* established.

35 Furthermore, the application of the principle *ne bis in idem* requires, in addition to the determination of a previous final decision (the so-called *bis* condition), also a two-stage examination of the identity of the facts and of the offender (the so-called *idem* condition).[40] Both identities are likely to exist frequently in cases of multiple sanctions for violations of Art. 10(1)(e) ESPR or, if applicable, also of Art. 6 GDPR. However, when examining the identity of the offender, it should be noted that the controller in the sense of Art. 4(7) GDPR and the processor in the sense of Art. 4(8) GDPR. will not necessarily coincide with the actors punishable for violations of Art. 10(1)(e) ESPR. Manufacturers who place products on the market or put them into service must, according to Art. 27(1)(c) ESPR, ensure that a DPP is available for the product in accordance with Art. 9 ESPR or with the corresponding delegated acts. Importers, in turn, may, according to Art. 29(2)(c) ESPR, only place products on the market that meet the same requirement. According to Art. 34 ESPR, the obligations for manufacturers can, under certain circumstances, also apply to distributors. Art. 9(1) ESPR, in its turn, explicitly refers to the fulfilment of the DPP-requirements in Art. 10 ESPR, which also include the data protection provision in Art. 10(1)(e) ESPR. Thus, within the framework of the ESPR, several actors (manufacturers, importers, and distributors) can simultaneously be held accountable for violations of Art. 10(1)(e) ESPR, even without them being subject to fines in the sense of the GDPR due to them eventually lacking the status of controllers or processors.

36 In the case of multiple sanctions against the same actor, the applicability of the principle of *ne bis in idem* will generally be established. Thus, double jeopardy (or even just renewed prosecution) would, in principle, be unlawful. Any exceptions to this would have to meet the relatively high hurdles of Art. 52(1) CFR: they would have to be provided for by law and be proportionate, respect the essence of the CFR, and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others. Since the legal interest protected by Art. 10(1)(e) ESPR is obviously the same as the one protected in Art. 6 GDPR (i.e., the protection of personal data), it is to be generally assumed that in the case of a simultaneous violation of both provisions, no exception to the principle of *ne bis in idem* according to Art. 52 CFR would be justified.

37 As a result, the applicable penalty for any violations of Art. 10(1)(e) ESPR (whether with or without a simultaneous violation of Art. 6 GDPR) is likely to depend heavily on which competent authority prosecutes the violation and which proceeding is concluded first. This unfortunate, uncertain legal situation is largely due to the fact that the ESPR, like the former Ecodesign Directive – and unlike the GDPR – has not established any concrete uniform standards for the imposition of sanctions. In this context, Art. 10(1)(e) ESPR is particularly problematic. For even if it could be argued to some extent that the different levels of penalties for violations of the ESPR would be justified by different weighing of the respective legal interests in the individual Member States, significant deviations between sanctions against violations of Art. 10(1)(e) ESPR and Art. 6 GDPR would hardly be justifiable; for in this case, both sanction frameworks are applicable *simultaneously* and in the *same Member State*. The applicability of different levels of penalties in this case is likely to constitute a violation of the principle of proportionality of the penalty (e.g., in the sense of Art. 49(3) CFR). This problem could be overcome by clearly defining under which specific circumstances which sanction framework is applicable. In this context, it would not seem unjustified to argue that, in the case of a simultaneous violation of Art. 10(1)(e) ESPR and Art. 6 GDPR, fines should only be imposed according to the milder penalty framework – generally, most likely that of the ESPR. This interpretation, although *in bonam partem*, leads to the paradox result that Art.

le società e la borsa (CONSOB) EU:C:2021:139, headnote 2; Markus Kubiciel and Gerson Großmann in Jürgen Meyer and Ulrich Hölscheidt (eds), *EU-Grundrechtecharta* (latest edn, Year) art 50 para 9; cf also Daniel Krause, 'Das Verbot der Doppelbestrafung (ne bis in idem, Art. 54 SDÜ, Art. 50 GRCh) bei Wirtschaftsstrafverfahren im Internationalen Raum mit Unternehmensbezug' (2025) *NStZ* 9, 14–15.

39 Cf eg Case C-857/19 *DB v Commissione nazionale per le società e la borsa (CONSOB)* EU:C:2021:139, headnote 2; Case C-117/20 *bpost SA v Autorité belge de la concurrence* EU:C:2022:202, headnote; Case C-151/20 *Nordzucker AG v Bundeskartellamt* EU:C:2022:203, headnote 1; cf also Daniel Krause, 'Das Verbot der Doppelbestrafung (ne bis in idem, Art. 54 SDÜ, Art. 50 GRCh) bei Wirtschaftsstrafverfahren im Internationalen Raum mit Unternehmensbezug' (2025) *NStZ* 9, 10–11.

40 The previous case law of the Court of Justice required, in competition law cases, as a third stage, the identity of the protected legal interests (cf eg Case C-857/19 *DB v Commissione nazionale per le società e la borsa (CONSOB)* EU:C:2021:139, para 43). This peculiar interpretation, which resulted in an unjustified special status of the principle *ne bis in idem* in competition law, was revised in March 2022 (Case C-117/20 *bpost SA v Autorité belge de la concurrence* EU:C:2022:202, para 35; Case C-151/20 *Nordzucker AG v Bundeskartellamt* EU:C:2022:203, para 39), and was confirmed in September 2023 (Case C-27/22 *AGCM v Ryanair DAC* EU:C:2023:139, para 67); cf also Martin Klusmann and Ole Schley, 'Einmal ist keinmal? Der EuGH und der Grundsatz *ne bis in idem*' (2022) *NZKart* 264, 266.

10(1)(e) ESPR, which obviously intended to provide special level of protection for customer data, instead makes the already high protection of the GDPR more flexible (by reducing the applicable penalty) and thus could, under certain circumstances, rather represent an *innovatio legis in melius* for controllers or data processors.

E. Concluding Remarks

38 Personal data concerning customers can be stored in a DPP in various scenarios. In these cases, the special protection provided by Art. 10(1)(e) must be observed, according to which such data may only be stored with explicit consent by the data subject. In this context, however, it seems appropriate to always consider the customer status *in connection with* the corresponding data storage in the DPP. This means that the special protection in Art. 10(1)(e) ESPR only applies to data that was stored because of or at least in direct connection with the customer status of the respective data subjects. This restrictive interpretation seems necessary to avoid unreasonable results in cases in which personal data of economic operators, DPP service providers or other actors in the DPP architecture is lawfully stored in the DPP on bases other than explicit consent, and these actors either simultaneously fulfil the conditions of the definition of customer or become a customer at a later date, which would result in the storing of their data being a violation of Art. 10(1)(e) ESPR.

39 In practice, due to the requirement of explicitness, high standards for the proof of consent are to be expected. Implied consent, although not to be excluded *a priori*, will generally not meet these requirements.

40 With regard to the applicable sanctions, the regulatory framework of the ESPR leads to major challenges with respect to the principle of *ne bis in idem*. Art. 10(1)(e) ESPR thereby leads to additional difficulties by the fact that violations of this provision could also constitute violations of Art. 6 GDPR, which makes it difficult to determine an applicable sanction framework. Insofar as no satisfactory solution seems to be found for this problem, one would expect that this issue will soon occupy the ECJ, and possibly also the European legislator.

Acknowledgment

This work was carried out as part of the project PASSAT (*Digital Product Passport Austria & Beyond*). This bilateral flagship project is funded in Austria by the Federal Ministry for Innovation, Mobility and Infrastructure (BMIMI) and the Austrian Research Promotion Agency (FFG), and in Germany by the Federal Ministry for Economic Affairs and Energy (BMWE) and the German Aerospace Centre – Project Management Agency (DLR-PT).