Computer Law & Security Review 60 (2026) 106251

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

If it ain't broke, don't fix it? Ten improvements for the upcoming tenth anniversary of the General Data Protection Regulation☆

Dariusz Kloza (ed.) [a,l,†,*], Laura Drechsler (ed.) [b,j,k], Elora Fernandes (ed.) [b], Arian Birth [c,l,†], Julien Rossi [d], Pierre Dewitte [b,e,††], Jarosław Greser [f], Lisette Mustert [g], Gianclaudio Malgieri [h], Heidi Beate Bentzen [i,†††]

[a] UCLouvain Saint-Louis Bruxelles (chargé de recherche FNRS), Belgium
[b] KU Leuven, Belgium
[c] Universität Greifswald, Germany
[d] Université Paris 8, France
[e] European Data Protection Supervisor, Belgium
[f] Uniwersytet Wrocławski, Poland
[g] Universiteit Utrecht, Netherlands
[h] Universiteit Leiden, Netherlands
[i] Centre for Medical Ethics, Universitetet i Oslo; Cancer Registry of Norway, Norwegian Institute of Public Health, Norway
[j] Open Universiteit, Netherlands
[k] Archives de l'État en Belgique / Rijksarchief in België / Belgisches Staatsarchiv, Belgium
[l] Van Bael & Bellis (VBB), Belgium

ARTICLE INFO

Keywords:
GDPR
Consent
Automated decision-making
Data protection by design
Data security
Data protection impact assessment
Data transfers – derogations
European Data Protection Board - dispute resolution
Data subjects – representation
Processing for scientific purposes

ABSTRACT

As the General Data Protection Regulation (GDPR) approaches its tenth anniversary, the European legislator is considering reforms thereto. This article offers a set of research-based suggestions for what such reforms could look like, based on two assumptions. First, that the GDPR is overall a solid piece of legislation that upholds the enduring objectives and principles of data protection law. Second, that any improvement cannot compromise the level of protection of fundamental rights currently offered. To this end, ten scholars from across Europe were invited to choose a provision of the GDPR, write about what works well and what does not, and why, as well as to suggest a solution for a concrete amendment of the text. The resulting wish-list discussing ten provisions (i.e., those concerning conditions for consent, children's consent, automated decision-making, data protection by design, data security, data protection impact assessment and prior consultation, derogations for data transfers, dispute resolution by the European Data Protection Board, representation of data subjects and processing for scientific purposes) is necessarily random and far from exhaustive. However, it lays the groundwork for a constructive debate, and we invite others to build on the list with their own proposals.

☆ Authors are listed according to their section contributions, except the first three, who also served as editors and appear first.

* Corresponding author.
E-mail addresses: dariusz.kloza@uclouvain.be, dkloza@vbb.com (D. Kloza), laura.drechsler@ou.nl, laura.drechsler@arch.be, laura.drechsler@kuleuven.be (L. Drechsler), elora.fernandes@kuleuven.be (E. Fernandes), s-arbirt@uni-greifswald.de, abirth@vbb.com (A. Birth), julien.rossi04@univ-paris8.fr (J. Rossi), pierre.dewitte@kuleuven.be (P. Dewitte), j.greser@greser.pl (J. Greser), l.mustert@uu.nl (L. Mustert), g.malgieri@law.leidenuniv.nl (G. Malgieri), h.b.bentzen@medisin.uio.no (H.B. Bentzen).

† This article contains solely my personal views and not those of any organisation I may be affiliated with.

†† This piece has been written in my capacity of research fellow at KU Leuven, and the views expressed do not reflect those of the European Data Protection Supervisor.

††† Views and opinions expressed are those of the author only and do not necessarily reflect those of the European Union, the European Innovation Council, or the Research Council of Norway. Neither the European Union nor the granting authorities can be held responsible for them.

https://doi.org/10.1016/j.clsr.2025.106251

Available online 23 January 2026

Introduction

A scholar once remarked that "very few legislative inventions get everything right first time around".[1] The General Data Protection Regulation (GDPR, the Regulation) is no exception.[2] Admitting that "it is occasionally necessary to change certain laws", another warned that the "law must be treated with trembling hands".[3] In the past months, first changes to the GDPR have been proposed using the narrative of "simplification" or increasing "competitiveness",[4] with further potential reforms on the horizon.[5]

This article offers a few research-based suggestions for how the GDPR could *actually* work better. These suggestions are based on two assumptions that are in contrast with the above narrative: first, that the GDPR is overall a solid piece of legislation that upholds the enduring objectives and principles of data protection law,[6] with only minor areas for improvement; second, that these improvements — aimed at, in particular, legal certainty, future-proofing, harmonisation (or: de-fragmentation) of internal market and administrative streamlining — cannot compromise the level of protection of fundamental rights, in particular the right to personal data protection, nor trigger an avalanche of deregulation.

As the GDPR approaches its tenth anniversary, the editors (DK, LD and EF) have asked a few scholars from across Europe — experts in their respective areas of data protection law — to reflect on what they would improve in the GDPR if they had the opportunity to do so. We invited them to choose a provision of the Regulation, and write about what works well, what does not and why, and to suggest a solution, at the same time estimating the gravity of their propositions (i.e., from a light review to a serious change). With this in mind, we also asked them to rewrite their selected provision. The resulting wish-list discussing ten provisions is necessarily random and far from exhaustive. We wish for such a constructive debate to continue, and we invite others to reflect on further GDPR provisions.

In this paper — essentially, a collection of short, standalone essays — each section is the sole responsibility of its author. We have refrained from offering any substantive guidelines to them and we have been exceptionally careful to allow them to express their ideas as they wished, with only minimal editorial intervention. Legal references and the jurisprudence quoted without any further specification relate to the GDPR and the Court of Justice of the European Union (CJEU), respectively.

A note on the understanding of the proposed rewritten provisions that are included in a box after each section: plain text indicates the original wording of a GDPR provision that the author has decided to keep. In turn, **bold text** indicates an added or rewritten provision. ~~**Bold text struck through**~~ or ***(Sentence repealed.)*** indicates a deleted part of a provision. Relatedly, if an entire (sub-)provision is deleted, this is marked by ***(repealed)***. In addition, a bracket ellipsis […] indicates that the original wording of a GDPR provision was not reproduced here, in the interest of space. Accordingly, included is only the core text of the amended provisions and omitted are the necessary changes in other parts of the Regulation. For example, if a new task for the European Data Protection Board (EDPB; the Board) is introduced, it should also be incorporated into Article 70(1) and Recital 139, although such an adjustment is not reproduced here. The text of any impacted national provisions is also not discussed.

Conditions for consent (Article 7)

Arian Birth

Improving legal certainty and streamlining the data subject's choice

Gravity of the proposed change: moderate

Introduction

Careful consideration as to how to protect data subjects ("end-users", on the grounds of the Digital Markets Act – DMA)[7] from harm resulting from the processing of their personal data reaches increased importance in nascent data-related legislation. Shortcomings of the GDPR have been (re)considered and addressed by recent legislative interventions, e.g., the DMA, which regulates services offered by gatekeepers. Article 5(2) DMA stipulates a four-point list of what gatekeepers must not do "unless the end user has been presented with the specific choice and has given consent". In parallel, Recital 37 DMA indicates a possibility for data subjects to choose an alternative service that might lack personalization, i.e., a "less personalized offer" where the essential quality of the core platform service remains unchanged. Since the DMA's approach is centred around "freely given" consent under Article 7(4), it is advisable to reconcile the codification consistently within the GDPR by incorporating the "less personalized alternative" into the conditions for valid consent. This amendment increases legal certainty not only by aligning the GDPR with the DMA but also by maturing the "take-it-or-leave-it" approach in the GDPR while simultaneously benefiting controller's GDPR compliance. The amendment also gives prominence to data subjects' decision-making about the processing of their personal data.

Scope of freely given consent under Article 7(4)

The GDPR clearly establishes that consent for processing of personal data must be "freely given" (Article 4(11)). This requires a genuine free choice by the data subject, including the ability to refuse consent

[1] Briggs A., *The Conflict of Laws* (5th ed., Oxford University Press 2024) 107 <https://doi.org/10.1093/oso/9780198895527.001.0001>.

[2] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 <http://data.europa.eu/eli/reg/2016/679/oj>.

[3] Montesquieu C., *The Persian Letters* (George R Healy tr., Hackett Publishing 1964 [1721]) 217 <https://archive.org/details/persianletters00montuoft>.

[4] Thus far, the GDPR has only been *corrected* three times, largely for linguistic and translation issues. The first ever proposal to slightly *amend* it was tabled in May 2025 (cf. European Commission, Proposal for a Regulation … amending Regulations … as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures, COM(2025) 501 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0501R%2802%29>). The GDPR is *supplemented* by Regulation 2025/2518 laying down additional procedural rules on the enforcement of Regulation (EU) 2016/679 [2025] OJ L 12.12.2025 <http://data.europa.eu/eli/reg/2025/2518/oj> (GDPR Procedural Regulation). This paper was written before the European Commission proposed on 19 November 2025 the Digital Omnibus Regulation aiming at another reform of the GDPR; cf. European Commission, Proposal for a Regulation ... amending Regulations ... as regards the simplification of the digital legislative framework ... (Digital Omnibus), Brussels, 19.11.2025, COM(2025) 837 final.

[5] Cf. e.g., Bertuzzi L., 'EU countries asked for their wish-list for 'simplification' of digital rules', MLex, 19 June 2025 <https://content.mlex.com/#/content/1662704/eu-countries-asked-for-their-wish-list-for-simplification-of-digital-rules>.

[6] Cf. Rossi J., 'La structure argumentative d'un demi-siècle de politique européenne de protection des données à caractère personnel' (2024) 81 Politique européenne 54 <https://doi.org/10.3917/poeu.081.0054>.

[7] Regulation 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1 <http://data.europa.eu/eli/reg/2022/1925/oj>.

without detriment,[8] i.e., without having to endure negative consequences.[9] For instance, refusal to consent cannot lead to a downgraded performance for the use of a service processing personal data.[10] Furthermore, "utmost account" must be taken that consent does not appear in a bundled or tied form (Article 7(4)).[11] Particularly, "unbundled" consent prevents that processing of personal data which is not necessary for the performance of the service is converged with the choice about necessary processing.[12]

Furthermore, Recital 42 clarifies that consent is not valid if the data subject has no genuine free choice. Naturally, the "take-it-or-leave-it" approach comes to mind, i.e., offering consent terms which are inappropriately broad in light of the performance of the service and whose refusal leads to the denial of access to the service. Such non-necessary processing must rather be rejectable for the data subject and not be presented as a binary choice of acceptance or refusal.[13] In essence, the condition requiring acceptance of unilaterally imposed (all-encompassing) processing terms to use a service is replaced by granularity, allowing selection between multiple processing operations. These range from relevant for the performance of a contract (i.e., fair terms), according to Article 7(4), to excessive ones which cannot influence the service access (i.e., unfair terms).[14] Nonetheless, unfair terms do not invalidate consent if they are clearly differentiated and data subjects can select them separately (i.e., sufficient granularity)[15] without having to accept them.[16] Contrarily, acceptance of fair terms, or in other words necessary processing, must lead to enjoyment of the service,[17] as clearly indicated in the EDPB Guidelines for Consent.[18] Controllers have the obligation to offer a granular selection under this scheme if they intend to rely on processing on the basis of consent, according to Article 6(1)(a).[19] Surprisingly, this distinction is not yet clearly outlined in the current Article 7(4), as proposed in the amendment. In fact, in Article 5(2) DMA and the DMA's Recitals, the legislator took the chance to provide further clarifications of consent to protect data subjects from unfair processing in large-scale digital platforms.

Less personalized alternative

At the outset, Article 5(2) DMA prevents certain processing operations listed exhaustively from occurring by default, unless data subjects give consent to those practices. Gatekeepers are obliged not to subject data subjects to processing operations that collect and/or combine personal data from various services offered in their digital ecosystem or source personal data from third-party services. Thereby, the DMA does not establish its own consent regime[20] and — according to Article 2(32) DMA and its Recital 37— refers to the GDPR's consent definition of Article 4(11). The referral to the GDPR is reiterated by Article 5(2) DMA, including a reference to the GDPR's Article 7.[21] Article 5(2) DMA also delimits the GDPR's lawfulness principle by excluding the listed processing operations to rely on performance of a contract (Article 6(1)(b)) and legitimate interest (Article 6(1)(f)). Consent thereby becomes the stellar lawful ground to process personal data outside (standalone) core platform services provided by a gatekeeper.

While it might not directly be apparent, this limitation follows the same logic as existent under the GDPR. The access to a (standalone) core platform service shall not be made conditional to the agreement to non-necessary processing operations which are not required in light of this service. In other words, gatekeepers cannot make access to services conditional on unfair processing terms under a "take-it-or-leave-it" option. Regardless of the foregoing, data subjects remain free to consent to processing beyond what is necessarily required (i.e., processing practices of Article 5(2) DMA) if they are entitled to a deliberate and free selection.

The GDPR to date conveyed this approach in a "mere" negative obligation pursuant to Article 7(4), outlining what a controller is not allowed to do. Comparatively, the DMA reaches beyond and formulates in Recitals 36 and 37 DMA a positive obligation that consent requires one proactively offered alternative which allows data subjects to freely choose non-necessary processing of personal data outside the core platform service or its functionalities without facing consequences in case of refusal.[22] Recital 36 DMA calls this a "less personalized but equivalent alternative" limited to necessary processing. Under this alternative, data subjects cannot be exposed to any different or degraded quality compared to the fully-personalized alternative[23] that contains not necessary processing of personal data.[24] Quality degradations are solely permitted for technical reasons, e.g., reduced personalized advertisement as a technical consequence of less collected and accurate

[8] Cf. Recital 42; Case C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt* ECLI:EU:C:2023:537 [2023] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0252> para. 143; EDPB, Guidelines 05/2020 on consent under Regulation 2016/679 (Version 1.0, 4 May 2020), paras. 3 and 5 <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en>; Bongartz P. and Kirk A., 'Art. 2 DMA' in Podszun R. (ed.), *Digital Markets Act* (1st edn, Nomos Beck Hart 2024), para. 149.

[9] EDPB (n 8), para 13; cf. Rauhofer J. and Schafer B., 'Art. 4(11) Consent' in Spiecker et al. (eds.), *General Data Protection Regulation*, (1st edn, Nomos Beck Hart 2023), para. 21.

[10] EDPB (n 8), para. 48.

[11] Geradin D. et al., 'The interplay between the Digital Markets Act and the General Data Protection Regulation' (2022) SSRN 9 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4203907>; Podszun R., 'Art. 5(2) DMA' in Podszun R. (ed.), *Digital Markets Act* (1st edn, Nomos Beck Hart 2024), paras. 23 and 24.

[12] EDPB (n 8), para. 32; Bongartz and Kirk (n 8), para. 149.

[13] EDPB (n 8), para. 37.

[14] Compare for the term "unfair" with Recital 42; cf. EDPB (n 8), para. 32; Podszun (n 11), para. 24; Rauhofer and Schafer (n 9), para. 29.

[15] EDPB (n 8), para. 44; Botta M., and Borges D., 'User Consent at the Interface of the DMA and the GDPR. A Privacy-setting Solution to Ensure Compliance with Art. 5(2) DMA' (2023) SSRN 16, 19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4650373>; Bongartz and Kirk (n 8), para. 150; Rauhofer and Schafer (n 9), para. 29.

[16] Botta and Borges (n 15) 18; Podszun (n 11), para. 23.

[17] Colangelo G., 'In Fairness We (Should Not) Trust: The Duplicitiy of EU Competition Policy Mantra in Digital Markets' (2023) 68(4) Antritust Bulletin 618, 619 et seq. <https://doi.org/10.1177/0003603X2312009>; Kerber W., and Zolna K., 'The German Facebook case: the law and economics of the relationship between competition and data protection law' (2022) 54 European Journal of Law and Economics 217, 240 <https://doi.org/10.1007/s10657-022-09727-8>.

[18] EDPB (n 8), para. 38. Cf. Bongartz and Kirk (n 8), para. 149; D'Amico A., 'Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be Freely Given?' (2023) 8(2) European Papers 611, 626 <https://doi.org/10.15166/2499-8249/678>.

[19] EDPB (n 8), para. 90.

[20] Geradin et al. (n 11) 8; Podszun (n 11), para. 10.

[21] Bongartz and Kirk (n 8), para. 147a.

[22] Botta and Borges (n 15) 17; Podszun (n 11), para. 24; Schmid C., and Späth C., 'Die weniger personalisierte Alternative nach Art. 5 Abs. 2 DMA – ein europäischer Sonderweg?' (2022) NZKart 568, 569.

[23] Geradin et al. (n 11) 10; Podszun (n 11), para. 24; Witt A., 'Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case' (2021) 66(2) Anitrust Bulletin 276, 295 <https://doi.org/10.1177/0003603X21997028>.

[24] Podszun R., 'Should gatekeepers be allowed to combine data? – Ideas for Art. 5(a) of the Draft Digital Markets Act' (2021) SSRN 10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3860030>; Podszun (n 11), para. 26.

personal data.[25] Henceforth, Article 5(2) DMA emphasizes preventive protection of personal data by default in accordance with Article 8 of the Charter of Fundamental Rights (CFR),[26] focusing on a self-determined choice of the data subject about the non-necessary disclosure of personal data.[27] Notably, Article 5(2) DMA coincides with the "take-it-or-leave-it" approach of the GDPR, precluding the bundling of unfair processing terms as an access condition for a service, in light of digital ecosystems.

Why is an adaption of Article 7(4) recommended?

First, the integration of the "less personalized alternative" in the GDPR resembles the consent standard under the "take-it-or-leave-it" approach as presupposed by GDPR caselaw and the EDPB Guidelines for Consent. Of utmost importance is that the CJEU in *Meta v. Bundeskartellamt* — even before *Meta* being subject to the obligations of Article 5 (2) DMA — held that systematic and all-encompassing processing of personal data, including data points accessed through third party digital service providers, under a conditional "take-it-or-leave-it" choice invalidates consent. To provide a GDPR-compliant consent option, the CJEU stated that a controller should offer at least one "equivalent alternative not accompanied" by non-necessary processing operations.[28] It comes without surprise that this case is considered to be the historic precedent for the regime of Article 5(2) DMA.[29]

Second, under the realization that the DMA follows the GDPR's consent regime by an explicit referral, there is indicative value that the legislator outlined the "less personalized alternative" with greater clarity without conceptually changing the pre-existing GDPR lawful ground of consent. If such a correlation is affirmed, there is also justification to ensure greater harmonisation and to take the inverse route by codifying the legal clarifications from Recitals 36 and 37 DMA in a similar manner into Article 7(4). Not to forget, that the codification within Article 7(4) would liberate the "less personalized alternative" from its concealed status in the DMA's recitals, although its long-standing existence of consent being "freely given". With the proposed amendment, the "take-it-or-leave-it" approach will be fixated in the GDPR's legislative text and made easily accessible for anyone, instead of being scattered across various sources. Alongside, this allows controllers and enforcement authorities to easily access the limitations and possibilities of consent.

Third, the risk of encountering bundled consent is presumably the highest in digital platforms which can easily scale non-necessary processing operations in light of the requested service by the data subject. While large-scale processing of personal data also entails a competitive advantage, the DMA – from its competition law angle – was predestined to provide a clarified consent standard.[30] However, a revised GDPR should not be limited to controllers in the digital sphere because various controllers can provide consent terms which entail non-necessary processing operations. For the data subject's control over their personal data, it is also irrelevant where unfair terms are encountered as long as the acceptance of excessive terms are the condition for accessing the service. The obligation to provide the "less personalized alternative" is instead triggered if Article 7(4) applies.[31]

Fourth, the codification provides a dogmatically reliable explanation why the lawfulness principle under Article 6(1)(a), contrary to all other lawful grounds for processing, does not entail a limitation of necessary processing. Although it is not unilaterally acknowledged that consent is deliberated from a necessity limitation,[32] the data subject's autonomous choice to allow processing of personal data beyond the merits of necessity respects their individual autonomy most, as long as this choice can indeed be exercised.[33] The proposed amendment allows consent for processing of non-necessary personal data, if this decision is based on a free and genuine choice of the data subject. Conversely, the data subject is protected from invasive processing by their right to personal data protection, allowing them to refuse processing beyond what is necessary. Altogether, the amendment focuses on the granular selection between necessary and non-necessary processing which reduces new ambiguity of the term "less personalized alternative". Yet, controllers keep control over the design of their services, which maintains a certain risk of willing or accidental inclusion of unfair terms into the "less personalized alternative". Unfortunately, this ambiguity cannot be entirely resolved because it would require regulating specific data processing operations contravening the technology-neutral objective of the GDPR.[34] Still, the clarification of what is permitted for consent will decrease possibilities to justify misconduct or differing interpretations.

Lastly, in light of the above, a clarification of "freely given" consent in Article 7(4) enhances legal certainty. Clearly outlined positive obligations in legal texts facilitate compliance efforts by guiding controllers how to structure consent requests and emphasizing required measures to be implemented by design, in accordance with Article 25(1). Instead, Article 7(4) – currently – solely states what must not be done, without clarifying what compliant consent should look like. The integration of the "less personalized alternative" also clarifies that non-necessary processing is not precluded for controllers as such, as long as the disclosure of more personal data is actually voluntary. This possibility is not entailed in the formulation of Article 7(4) yet,[35] although it has already been permitted. After all, the right to personal data protection is presumably protected to a further extent if the consent request compiles equal alternatives across different controllers, allowing data subjects to

[25] Quality might be assessed from different angles, it can be considered that a higher degree of personalization is quality enhancing, compare Botta and Borges (n 15) 18; Frank M., and Lewis E., 'The European Commission's Challenge to Consent or Pay: Demystifying the Digital Markets Act?' (2024) 47(4) World Competition 427, 440 <https://doi.org/10.54648/woco2024026>.

[26] Charter of Fundamental Rights [2012] OJ C326 <https://eur-lex.europa.eu/eli/treaty/char_2016/oj>.

[27] D'Amico (n 18) 612; Hornung G., and Spiecker I., 'Art. 1 Subject Matter and Objectives' in Spiecker et al (eds), *General Data Protection Regulation* (1st edn, Nomos Beck Hart 2023), para. 27; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 [2014] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293> paras. 27, 33 and 37; Joined Cases C-511/18, C-512/18 and C-520/18 *Le Quadrature du Net* ECLI:EU:C:2020:791 [2020] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0511> para. 117.

[28] Case C-252/21 *Meta v. Bundeskartellamt* (n 8), para. 150.

[29] Geradin et al. (n 11) 218; Podszun (n 11), para. 12; cf. Witt (n 23) 281.

[30] The compelling need to eventually clarify the "less personalized alternative" in the DMA is the pertinent risk of large-scale digital ecosystem with their far-reaching services that allow non-necessary processing of personal data in a multitude of occasions. Cf. Rauhofer and Schafer (n 9), para. 42.

[31] Cf. EDPB (n 8), paras. 32 and 33, entailing the example that a bank is asking its customers to provide their payment details for direct marketing purposes, which is logically not required for the provision of a bank account.

[32] For a comprehensive illustration of consent criticism, cf. Sartor G., 'Art. 6 Lawfulness of processing' in Spiecker et al (eds.), *General Data Protection Regulation* (1st edn, Nomos Beck Hart 2023), paras. 22-30.

[33] Kirk A., 'Consumer Autonomy and the Charter of Fundamental Rights' (2024) 13(4) EuCML 170, 171; Rauhofer and Schafer (n 9), para. 8.

[34] Cf. Hornung G., and Spiecker I., 'Introduction: General aims and principles of data protection law' in Spiecker et al (eds.), *General Data Protection Regulation* (1st edn, Nomos Beck Hart 2023), para. 192 with further references to advantages and disadvantages.

[35] This naturally requires the compliance with other principles of Article 5.

make a deliberate choice and control to refuse certain data processing operations.

Article 7
Conditions for consent
[…]
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. **The data subject may genuinely and freely choose to accept the processing of personal data that is not necessary for the performance of the contract.**
5. **Where Article 7(4) applies, another less personalized but equivalent alternative, entailing only necessary processing of personal data, shall be proactively offered to the data subject to ensure that processing which is not necessary can be refused, if applicable, without suppressing the functionalities of the service, unless any resulting degradation is a direct consequence of the inability to process personal data that is not necessary for the performance of a contract.**

Conditions applicable to child's consent in relation to information society services (Article 8)

Elora Fernandes
Embedding children's best interests in all data processing activities
Gravity of the proposed change: serious

Introduction

Representing a significant advancement over the Data Protection Directive (DPD),[36] Article 8 seeks to balance children's status as rights holders with their developing capacity to make informed decisions in the digital environment. By establishing special requirements for consent up to a certain age, the provision reflects an understanding that children are more vulnerable and often lack full awareness of risks, consequences and safeguards related to data processing, as well as of their rights as data subjects.[37] This aligns with the European Union (EU)'s commitment to protecting the rights of the child, as laid down in Article 3(3) of the Treaty on European Union (TEU) and Article 24 CFR. Article 8, however, is only focused on consent, which represents a rather simplistic approach *vis-à-vis* the broader need to safeguard children's fundamental rights in data processing activities. Article 8, therefore, presents some shortcomings that could be addressed to *enhance* the protection and promotion of children's rights in the digital environment, ensuring that the regulation keeps pace with evolving risks and continues to serve their best interests.

Age of consent

Article 8(1) defines the age of consent (13 to 16 years old) required for processing children's personal data under Article 6(1) when offering information society services (ISS) directly to a child. This provision presents five main challenges, which are discussed below.

First, the age of consent requirement currently applies only when consent as a lawful basis under Article 6(1) is relied upon, which may leave a gap in protection when special categories of data are processed. In theory, any lawful ground of Article 6(1) could be used in tandem with explicit consent under Article 9(2)(a). This highlights the need to extend Article 8(1) to cover all situations where consent is used for processing children's data, be it as a legal basis under Article 6(1) or as a condition for processing special categories of data under Article 9(2)(a). The requirement for *explicit* consent is also proposed to apply to all instances of processing of children's data, given their enhanced vulnerability and the need for higher control over personal data.

Second, the current wording of Article 8(1) limits its application to ISS, as defined in Article 4(25) (which refers to Directive 2015/1535).[38] This narrow scope lacks justification, as many risky data-driven services used by or significantly impacting children may fall outside that definition. Important examples include the use of biometric systems (which may not be considered services offered "at a distance") or educational technologies (which may not be considered provided "at the individual request", given that schools are the ones procuring the service). In theory, controllers that are not providers of ISS, and to whom Article 8 would not apply, must rely on national laws governing the legal capacity of children and/or assess, on a case-by-case basis, whether the child has the maturity to provide valid consent in accordance with Article 4(11). Broadening the provision to encompass all situations where children's data are processed would, therefore, create a technology-neutral and less fragmented framework across all contexts.[39] Removing this requirement would also eliminate the ambiguity around the need for an ISS to be provided directly to a child for the provision to apply — a condition that must be broadly interpreted to avoid limiting it to services *exclusively* designed for children.[40]

Third, determining the appropriate age at which certain rights are granted or protections withdrawn is a complex issue.[41] A child's readiness for decision-making and self-responsibility is always best assessed not by chronological age alone, but by context.[42] Given the need for legal certainty and predictability, though, establishing an age threshold *ex ante* is sometimes necessary. As a rule, all EU Member States set the age of majority at 18 for civil acts. However, especially when these are linked to non-patrimonial rights, exceptions can be made by law. This occurs in some Member States, for instance, regarding consent to medical treatment, engagement in sexual activities, voting, or adoption.[43] In such circumstances, however, by interpreting the best interests principle as a rule of procedure, policy- and law-makers are required to assess the impact of any provision on children's rights, drawing on empirical evidence and guided by a precautionary approach.[44]

The impact assessment accompanying the GDPR acknowledges that

[36] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 <http://data.europa.eu/eli/dir/1995/46/oj>.
[37] Recitals 38 and 75.
[38] Directive 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) [2015] OJ L241/1 <http://data.europa.eu/eli/dir/2015/1535/oj>.
[39] The first draft of the Commission's proposal for the GDPR, leaked in 2011, introduced a broader rule for parental consent that applied to all processing activities involving children up to the age of 18 (cf. <https://www.statewatch.org/media/documents/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf>). Broadening the scope of this provision was also suggested by Article 29 Working Party (WP29) in its Opinion on the reform that led to the GDPR. WP29, 'Opinion 01/2012 on the data protection reform proposals' (23 March 2012) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf>.
[40] Cf. the EDPB's understanding on "offered directly to a child": EDPB (n 8).
[41] UNICEF, 'Implementation Handbook for the Convention on the Rights of the Child' (2007) <https://www.unicef.org/reports/implementation-handbook-convention-rights-child>.
[42] Cannataci J., 'Artificial Intelligence and Privacy, and Children's Privacy. Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci. A/HRC/46/37' para. 114 <https://documents.un.org/doc/undoc/gen/g21/015/65/pdf/g2101565.pdf?OpenElement>.
[43] European Union Agency for Fundamental Rights (FRA), 'Mapping minimum age requirements concerning the rights of the child in the EU' (20 November 2017) <https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu>.
[44] Committee on the Rights of the Child, 'General Comment No. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (Art. 3, Para. 1). CRC/C/GC/14' (United Nations 2013) <https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf>.

the age of consent was directly inspired by the United States (US)' Children's Online Privacy Protection Act (COPPA) of 1998.[45] According to the European Commission, this alignment was intended to benefit online businesses by avoiding "undue and unrealistic burdens upon providers of online services and other controllers".[46] This choice presents two main problems. First, it relies on a foreign legal framework that was not developed with the specific interests of EU children or sovereignty in mind. Second, COPPA's own age of consent threshold was not based on scientific evidence but rather emerged from political compromise.[47]

Within the EU, research shows that 43 % of eighth-grade students (aged 13–14) still have only limited digital skills. Skills related to commercial literacy (which are particularly relevant for assessing a child's capacity to provide informed consent under the current wording of Article 8(1)) are primarily found at Level 4 of the International Computer and Information Literacy Study (ICILS) 2023 proficiency framework.[48] However, this level was not achieved on average across EU Member States. Results also widely varied between countries, which reveals significant inconsistencies in digital literacy across the region.[49] Empirical research assessed by Livingstone and Ólafsson indicates that children's commercial literacy, particularly in the UK, steadily increases from around age eight into young adulthood, with a significant leap observed between the ages of 12 and 15.[50] More broadly, windows of developmental sensitivity have been found to vary between boys (14–15 years) and girls (11–13 years) depending on maturational processes.[51] This suggests that setting the minimum age of digital consent at 13 may be premature for many children across the EU and does not reliably reflect actual readiness for informed decision-making.

Beyond the question of choosing the appropriate age of consent, the effective protection of children is further undermined by a lack of consistency across the EU, with Member States adopting all age options allowed for under Article 8(1).[52] This fragmented implementation is said to make compliance more complicated for controllers operating across borders[53] (though this is mostly an automated exercise when it comes to larger players), and raises concerns about unjustified disparities among children in different Member States.[54]

To address both the need for aligning the age of consent with existing scientific evidence on children's evolving digital literacy and to strengthen the GDPR's goal of harmonization, the amendment adopts a uniform age of 16 as the sole threshold across Member States. In a more concrete scenario of possible change of the regulation, however, further and specific research would ideally be carried out to assess the real impact of this decision on EU children across contexts and regions.

Fourth, considering children's right to have their view given due weight according to their age and maturity (Article 12 of the Convention on the Rights of the Child – CRC), the need to balance provision, participation and protection rights,[55] as well as the fact that adults also struggle to make such judgment calls,[56] an assistance mechanism is proposed. This is inspired by the regime existent in civil law countries, whereby as of a certain age consent needs to be given by both the minor and the legal guardian for an act of civil life to be valid, especially when this affects personality rights. This joint-consent model already exists in the French data protection law,[57] which acknowledges the child's right to participation while preserving the protective role parents or guardians could play. The amendment also aligns with the need that decisions made by holders of parental responsibility be in the best interests of the child and, importantly, involve the *actual* data subject in the process as much as possible, thereby enhancing digital literacy from an early age.

Fifth, and finally, in cases where consent decisions are initially made by the holder of parental responsibility, children have limited control over their personal data — even though they could, in theory, withdraw consent given on their behalf.[58] Given that children may not be fully

[45] United States of America, Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. 6501–6505.

[46] European Commission, 'Impact Assessment, Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data' (2012) 68 <https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf>. See also: Council of the European Union, 'Interinstitutional File: 2012/0011 (COD): Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' (2014) para. 87 <https://www.statewatch.org/media/documents/news/2014/jul/eu-council-dp-reg-11028-14.pdf>.

[47] Macenaite M., and Kosta E., 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26 Information and Communications Technology Law 146 <https://doi.org/10.1080/13600834.2017.1321096>.

[48] IEA, 'International Computer and Information Literacy Study' <https://www.iea.nl/studies/iea/icils>.

[49] European Commission, Directorate-General for Education, Youth, Sport and Culture, 'International Computer and Information Literacy Study (ICILS) in Europe, 2023 – Main findings and educational policy implications' (Publications Office of the European Union, 2024) <https://data.europa.eu/doi/10.2766/5221263>.

[50] Livingstone S., and Ólafsson K., 'Children's Commercial Media Literacy: New Evidence Relevant to UK Policy Decisions Regarding the GDPR' (Media@LSE, 26 January 2017) <https://blogs.lse.ac.uk/medialse/2017/01/26/childrens-commercial-media-literacy-new-evidence-relevant-to-uk-policy-decisions-regarding-the-gdpr/>.

[51] Marciano L. et al., 'Digital Media, Cognition, and Brain Development in Adolescence' in Christakis D., and Hale L. (eds), *Handbook of Children and Screens: Digital Media, Development, and Well-Being from Birth Through Adolescence* (Springer 2025) 22.

[52] Milkaite I., and Lievens E., 'Status Quo Regarding the Child's Article 8 GDPR Age of Consent for Data Processing across the EU' (Better Internet for Kids, 20 December 2019) <http://hdl.handle.net/1854/LU-8640119>.

[53] The age of a child's consent was one of the main points of fragmentation raised by stakeholders, as reported by the European Commission in its Second Report on the application of the GDPR. European Commission, 'Communication from the Commission to the European Parliament and the Council. Second Report on the application of the General Data Protection Regulation' (2024), COM/2024/357 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2024%3A357%3AFIN&qid=1721897017650#footnote71>.

[54] Milkaite I., 'A Children's Rights Perspective on Privacy and Data Protection in the Digital Age: A Critical and Forward-Looking Analysis of the EU General Data Protection Regulation and Its Implementation with Respect to Children and Youth' <http://hdl.handle.net/1854/LU-8714018>.

[55] Livingstone S., and O'Neill B., 'Children's Rights Online: Challenges, Dilemmas and Emerging Directions' in van der Hof S. et al (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety* (Springer 2014).

[56] Van Der Hof S., 'I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2017) 32 Wisconsin International Law Journal 409.

[57] Article 7-1, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cf.: Commission Nationale de l'Informatique et des Libertés (CNIL), 'Recommendation 4: Seek Parental Consent for Children under 15' (9 August 2021) <https://www.cnil.fr/en/recommendation-4-seek-parental-consent-children-under-15>.

[58] According to the EDPB's guidelines on consent, if a child takes no action, consent previously given or authorized by a holder of parental responsibility before reaching the age of digital consent remains valid (para. 148). Nonetheless, the controller must inform the child of their right to withdraw consent (para. 149). Cf. EDPB (n 8).

aware of all instances in which such consent was granted, this could be remedied if controllers would seek renewed consent once the child reaches the appropriate age.[59] This ensures that the individual, now presumed capable of making better decisions (even if they have previously given joint consent as a child), is provided with a meaningful opportunity to reaffirm or withdraw consent.

Age assurance mechanisms

In its current form, the GDPR does not explicitly mandate the implementation of age assurance mechanisms. Often, however, these mechanisms can be considered as an implicit requirement.[60] They can be crucial as (i) a way to guarantee the lawfulness of certain acts, such as proving the validity of a contract, an essential element for relying on Article 6(1)(b) as a legal basis, or of consent; as well as (ii) a measure to comply with other obligations, such as with the principles of purpose limitation and data minimization. The amendment has the sole purpose to clarify that age assurance mechanisms are not merely implied, but constitute an explicit obligation under the GDPR when assessing the validity of consent. Given the wide range of possible approaches (from self-declaration to age estimation and age verification),[61] determining what is appropriate must be assessed on a case-by-case basis. Accordingly, this evaluation should remain part of the measures to be adopted considering the criteria established in Articles 24(1) and 25(1), as well as the specific guidance from the EDPB,[62] for both objectives of age assurance specified above.

The best interests of the child principle as a vector for the precautionary approach

Introducing an age of consent is not sufficient to truly safeguard children's right to data protection, both as an end in itself and as a means to promote other fundamental rights. This approach is still grounded in a static view of childhood and development,[63] which should be complemented by a dynamic perspective.[64] This recognizes the evolving capacities of the child and the need to proactively involve families, as well as public and private entities, in the *promotion* of children's rights (not only *protection* rights, but also *participation* and *provision* rights).[65] This could be achieved by defining specific obligations for controllers to provide more concreteness of Recital 38.

Therefore, the amendment includes a more general provision mandating that the processing of children's data be always aligned with their best interests. This possibility had already been raised by some Member States during the discussions in the Council at the time of the GDPR proposal, but did not make it to the final text.[66] The amendment further incorporates a definition of a child in Article 4(1), aligning it with the one in the CRC and with the age of majority in EU Member States. Similarly, this was also present in the GDPR proposal but was excluded throughout the legislative process.

Article 24 CFR and Article 3(1) CRC state that children have the right to have their best interests taken as a primary consideration in all actions that concern them, either by public or private actors. The contours of this principle were first elaborated by the Committee on the Rights of the Child in its General Comment No. 14 of 2013.[67] While it does not attempt to prescribe what is in the best interest of a child in any given situation, it provides a framework for identifying it in a concrete case. The principle has three main roles: as a fundamental right, as an interpretative principle, and as a rule of procedure. The Committee identifies children's rights impact assessments (CRIAs)[68] as the most effective tool for determining and balancing the rights of the child in a given decision, particularly when they may conflict — for example, the right to education and the right to data protection. Once the child's best interests are established, they may be weighed against third-party interests.[69] However, the child's interests must be given *primary consideration* rather than being treated as just one factor among many.

Given children's special status as data subjects, the best interests of the child principle closely aligns with a precautionary approach.[70] This means that controllers must consider not only the risks of clearly defined harms in their assessment, but also to *plausible* harms supported by reasonable evidence. This approach is already recognized, for instance,

[59] The right to erasure is particularly important in these cases, especially when the data subject, now an adult, does not agree with the consent given on their behalf (Recital 65).

[60] European Commission: Directorate-General for Communications Networks, Content and Technology, Shaffique MR and Hof S van der, 'Mapping Age Assurance Typologies and Requirements – Research Report' (Publications Office of the European Union 2024) <https://data.europa.eu/doi/10.2759/455338>.

[61] Sas M. and Mühlberg J., 'Trustworthy Age Assurance? A Risk-Based Evaluation of Available Und Upcoming Age Assurance Technologies from a Fundamental Rights Perspective' (The Greens/EFA in the European Parliament 2024) <https://www.greens-efa.eu/files/assets/docs/age_assurance_v2.1.pdf>.

[62] European Data Protection Board (EDPB), 'Statement 1/2025 on Age Assurance' (2025) <https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-12025-age-assurance_en>.

[63] See Livingstone S., and Sylwander K., 'There Is No Right Age! The Search for Age-Appropriate Ways to Support Children's Digital Lives and Rights' (2025) 19 Journal of Children and Media 6 <https://doi.org/10.1080/17482798.2024.2435015>.

[64] This was also the opinion of WP29: "From the static point of view, the child is a person who has not yet achieved physical and psychological maturity. From the dynamic point of view, the child is in the process of developing physically and mentally to become an adult. The rights of the child, and the exercise of those rights – including that of data protection, should be expressed in a way which recognises both of these perspectives." WP29, 'Working Document 1/2008 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)' (18 February 2008) 3 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf>.

[65] Much of children's vulnerability comes not only from their developmental stage and limited of capacity to make appropriate decisions, but also from the legal implications of this recognition, i.e., their lack of power to exercise their rights and challenge abuses. Lansdown G., 'The Evolving Capacities of the Child' (Save the Children; UNICEF 2005) 32 <https://digitallibrary.un.org/record/556609?v=pdf>.

[66] Council of the European Union (n 46) 87 (footnote 85).

[67] Committee on the Rights of the Child (n 44) para. 74.

[68] Cf. Mukherjee S., Pothong K., and Livingstone S., 'Child Rights Impact Assessment: A Tool to Realise Children's Rights in the Digital Environment' <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/03/CRIA-Report.pdf>; Dutch Ministry of the Interior and Kingdom Relations (BZK), 'Child Rights Impact Assessment (Fillable Form)' <https://www.nldigitalgovernment.nl/document/childrens-rights-impact-assessment-fill-in-document/>.

[69] See, for instance, the use of legitimate interest as a lawful basis for processing children's data: Fernandes E. et al., 'Contribution to the Public Consultation on EDPB Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR: Points of Attention Regarding the Processing of Children's Data' (2024) <https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=alma9995078251301488&context=L&vid=32KUL_KUL:KULeuven&search_scope=All_Content&tab=all_content_tab&lang=en>.

[70] Lievens E., 'Growing Up with Digital Technologies: How the Precautionary Principle Might Contribute to Addressing Potential Serious Harm to Children's Rights' (2021) 39 Nordic Journal of Human Rights 128 <https://doi.org/10.1080/18918131.2021.1992951>.

in the Audiovisual Media Services Directive (AVMSD).[71] Moreover, the assessment should account not only for immediate, but also for medium- and long-term effects that might affect children's rights over time.[72]

Considering the open-ended nature of the best interests of the child principle,[73] it is important to define red lines, as well as a clear mandate for the EDPB to elaborate on grey areas. On the former, the two examples of criteria mentioned above can provide some direction. While Article 28(2) of the Digital Services Act (DSA)[74] prohibits online platforms to present advertisements on their interface based on the profiling of minors (which could already be said to be prohibited for other controllers as well),[75] there is already enough evidence on the interdisciplinary literature,[76] as well as calls by the Council of Europe[77] and the Committee on the Rights of the Child,[78] about the risks that commercial profiling as a whole pose to children. The amendment therefore aims to address this issue through a broader prohibition, while also providing more concreteness to Recitals 38 and 71.

A best-interests-based precautionary approach would also strengthen existing requirements under the GDPR, such as data protection by design, tailoring them to the specific needs of children. This is already reflected in certain Data Protection Authorities' (DPA) guidelines on the topic — most notably the Irish Data Protection Commission's (DPC),[79] which draws significant inspiration from the United Kingdom (UK) Information Commissioner's Office's (ICO) Age-Appropriate Design Code.[80]

Article 4
Definitions
[…]
(27) 'Child' means any person who is under 18 years of age;

Article 8
Conditions applicable to child**ren's data processing** ~~consent in relation to information society services~~

1. Where point (a) of Article 6(1) **or point (a) of Article 9(2)** applies ~~in relation to the offer of information society services directly to a child,~~ the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that **explicit** consent is given or authorised by the holder of parental responsibility **jointly with** the child**, in accordance with the child's evolving capacities**.
~~Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.~~
2. ~~The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology~~. **In accordance with Article 25(1), the controller shall adopt appropriate measures to implement effective age assurance mechanisms enabling the determination of whether joint parental consent is required, as well as to ascertain that such consent has been validly given by the holder of parental responsibility and the child.**
2a. Upon the data subject reaching the age of 16, the controller shall obtain renewed consent from the data subject to confirm any prior consent granted by a holder of parental responsibility jointly with the child. The data subject shall retain the right to request the rectification or erasure of their personal data, irrespective of the fact that they are no longer a child.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.
4. The processing of personal data relating to a child shall be guided by their best interests, which must be a primary consideration in all decisions taken by controllers and processors. The best interests of the child in any data processing activity shall be identified through a children's rights impact assessment.
5. The profiling of children for direct or indirect commercial purposes shall be prohibited, unless it is demonstrably in the child's best interests. Profiling for the purpose of targeted advertising, behavioural manipulation, emotional

(*continued on next page*)

[71] See, for instance, Article 6a(1) and Article 28b(1)(a) AVMSD, respectively (emphasis added): "Member States shall take appropriate measures to ensure that audiovisual media services provided by media service providers under their jurisdiction which *may impair* the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them"; "1. Without prejudice to Articles 12 to 15 of Directive 2000/31/EC, Member States shall ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect: (a) minors from programmes, user-generated videos and audiovisual commercial communications which *may impair* their physical, mental or moral development in accordance with Article 6a(1)."

[72] Committee on the Rights of the Child (n 44).

[73] Collinson J. and Persson J., 'What Does the "Best Interests of the Child" Mean for Protecting Children's Digital Rights? A Narrative Literature Review in the Context of the ICO's Age Appropriate Design Code' (2022) 27 *Communications Law* 132.

[74] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) 2022 (OJ L 277) 1.

[75] In relation to targeting advertisement, the WP29 emphasized that "data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing". WP29, 'Opinion 02/2013 on Apps on Smart Devices' <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>. The EDPB reiterated this view in the endorsed WP29 guidelines on automated individual decision-making and profiling, stating that organizations should refrain from profiling children for marketing purposes, as this would reach the threshold of significant effects on data subjects imposed by art. 22. WP29, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2016) 21 <https://ec.europa.eu/newsroom/article29/items/612053/en>.

[76] For an up-to-date and comprehensive literature review on the risks of commercial profiling to children, as well as a taxonomy of commercial profiling, see: Leijten E. and Van Der Hof S., 'Dissecting the Commercial Profiling of Children: A Proposed Taxonomy and Assessment of the GDPR, UCPD, DSA and AI Act in Light of the Precautionary Principle' (2025) 57 Computer Law & Security Review 106143 <https://linkinghub.elsevier.com/retrieve/pii/S2212473X25000161>.

[77] "Profiling of children, which is any form of automated processing of personal data which consists of applying a "profile" to a child, particularly in order to take decisions concerning the child or to analyse or predict his or her personal preferences, behaviour and attitudes, should be prohibited by law. In exceptional circumstances, States may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law". Council of Europe, Committee of Ministers, Recommendation CM/Rec(2018) 7 of the Committee of Ministers to Member States on Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (2018) para. 37 < https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808b79f7>.

[78] "States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children". Committee on the Rights of the Child, 'General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment. CRC/C/GC/25' para. 42 <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>.

[79] DPC, 'Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing' <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>.

[80] ICO, 'Age Appropriate Design: A Code of Practice for Online Services' <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>.

(*continued*)

analytics, or similar commercial practices shall not be regarded as being in the child's best interests.

6. The Board referred to in Article 68 shall issue guidelines on the implementation of the best interests of the child principle in the context of data processing. Such guidelines shall address, inter alia, appropriate methodologies for conducting a children's rights impact assessment and its interplay with data protection impact assessment referred to in Article 35; the deployment of age assurance technologies; age-appropriate design standards; guidance on the exercise of data subjects rights by children; and mechanisms for transparent and child-friendly communication.

Automated individual decision-making, including profiling (Article 22)

Julien Rossi
Towards a meaningful human intervention in automated decision-making
Gravity of the proposed change: light

Article 22: A convoluted script to regulate ADM

The automation of decision-making can be a direct challenge to the nature of law as we conceive it in both common law and continental law systems. To be binding, legal norms must first and foremost, be public and intelligible; computer programs supporting automated decision-making (ADM) are often not. Binding decisions are supposed to be justified on such public legal rules, so that they can then be challenged. And the law is normative. Judges — and legal decision-makers in general — do not only apply descriptive precedent. They interpret a complex set of positive rules to concrete cases by determining what behaviour should be allowed according to them; not based on what behaviour was previously allowed and baked into an algorithm.[81] They are then able to *justify* their decision, and legal decision-makers can be held accountable, whereas when they can blame machines for unfair or unfounded decisions, this leads to "agency laundering",[82] a situation where blame is shifted onto a machine. This can lead to significant harm on both individual and collective level.

The prohibition of ADM was, therefore, one of the first rules introduced in French data protection law. Following the worries expressed in 1970 by the State Council on the consequences of computers in public administration on civil liberties,[83] it was included in Article 2 of the 1978 Law on Computers, Files and Freedom[84] by the French legislator, which presented it as a clear prohibition. In 1995, however, the European legislator chose to translate this into a more ambiguous formula in its DPD, creating a "right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data" (Article 15 DPD). This kind of convoluted formula was kept in the GDPR, which states, in its Article 22(1), that the "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". Does this amount to a clear prohibition, as claimed by the European DPAs?[85] Or, as Moral Soriano puts it, does it merely "[assemble] a set of guarantees that must be provided to protect citizens against decisions using ADM systems"?[86] At first sight, there is indeed quite a large amount of ambiguity in this provision, derived from the way in which it was coined by the legislator.[87] Based on both the genealogy of this provision, and on textual analysis, the latter interpretation seems to be the most likely.[88] In practice, this does not arguably create a huge difference with what a general ban on automated decision-making would have made. Indeed, Article 22 creates, in almost all cases, a right to *object* to ADM, and a right to an explanation (if not to a justification).

Article 22 creates a clear right to be informed and to object

First, Article 22 makes it clear that a data subject always has a right to object to any decision producing legal effects or that "significantly affects him or her". There are exceptions. One is when it is "is necessary for entering into, or performance of, a contract between the data subject and a data controller" (Article 22(2)(a)), another is with the data subject's explicit consent (Article 22(2)(c)). In both cases, Article 22(3) gives the "right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision". This basically amounts to negating the effects of the exception to the general right to object to ADM expressed in paragraph 1. This is reinforced by the fact that the exception, where consent can provide for a legal basis for ADM, can only exist if it is an exception used to authorise something which is otherwise banned to begin with.

A third exception is when ADM is "authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests" (Article 22(2)(b)). This means that the GDPR allows Member States to negate data subjects' rights to object to decisions based solely on ADM, even though there would still be a possibility to contest that measures provided for in national law do not meet the standards of EU law, including those set forth in the CFR, in addition to protections afforded by national constitutional law. This would necessarily imply the right to a fair trial and to legal remedy when confronted with an illegal decision made by means of ADM, and a right to an explanation.

Indeed, Article 22 must be read in combination with Article 15(1)(h), which gives a right to "meaningful information about the logic involved [in the ADM process], as well as the significance and the envisaged consequences of such processing for the data subject". This has a rather broad scope, as even the establishment of a credit score — not even the actual decision to grant or deny a loan — falls under the scope of this provision as soon as this score is a determining factor in the actual decision.[89] And, in line with the importance of being able to access legal sources in an understandable manner, the CJEU has also ruled that rules protecting intellectual property or trade secrets cannot be used to systematically refuse any explanation as to the logic involved in reaching

[81] Moral Soriano L., 'Right Not to Use the Internet: Lessons to Be Learned from the Right Not to Be Subject to Automated Decisions' in Kloza D. et al. (eds.), *The Right Not to Use the Internet. Concepts, Contexts, Consequences* (Routledge 2025) <https://doi.org/10.4324/9781003528401>.

[82] Rubel A. et al., 'Agency Laundering and Information Technologies' (2019) 22 Ethical Theory and Moral Practice 1017 <https://doi.org/10.1007/s10677-019-10030-w>.

[83] Conseil d'Etat, 'Les Conséquences Du Développement de l'informatique Sur Les Libertés Publiques et Sur Les Décisions Administratives' (1970).

[84] Loi 78-17 (n 57).

[85] WP29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (6 February 2018) 19 <https://ec.europa.eu/newsroom/article29/items/612053>.

[86] Moral Soriano (n 81) 145.

[87] Tosoni L., 'The Right to Object to Automated Individual Decisions: Resolving the Ambiguity of Article 22(1) of the General Data Protection Regulation' (2021) 11 International Data Privacy Law 145 <https://doi.org/10.1093/idpl/ipaa024>.

[88] Ibid.

[89] See, i.a. Cases C-487/21, *FF v Österreichische Datenschutzbehörde* ECLI:EU:C:2023:369 [2023] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0487> and C-634/21, *OQ v Land Hessen* ECLI:EU:C:2023:957 [2023] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0634>.

the automated decision.[90] This follows another decision, on the accessibility of harmonised standards that actually form part of EU law.[91] The logic behind those decisions remains the same: rules that have binding legal effects or significantly affect someone must be transparent and subject to either public (in the case of harmonised standards) or individual (in individual ADM cases) scrutiny.

The transparency obligations are further reinforced when ADM relies on high-risk artificial intelligence (AI) systems as defined under the Artificial Intelligence Act (AI Act).[92] Its Article 86 indeed creates a right to an explanation to decisions taken by deployers of such high-risk AI systems.[93] The interplay with Article 22 is not very clear, as Article 86(3) of the AI Act states that its right to an explanation "shall apply only to the extent that [it] is not otherwise provided for under Union law". As such, it should be interpreted as complementing Article 22 in case the latter does not cover, which includes at least cases where affected persons are not individuals but legal persons, such as companies.

Both the right to object to ADM and the right to an explanation are therefore fairly well protected, meaning data controllers must — except in some rare cases provided for in national law where this would still not clash with other fundamental rights — always maintain decision-making processes based on human cognition at least in parallel with ADM.

What does a right to human intervention look like?

The editors of this article are right to warn of the high risks of opening the GDPR to amendments at this point. A high degree of caution must always be exercised when changing the law, especially when touching upon rules that have existed for decades and appear to have been highly adaptable to technological change. Regarding Article 22, this is especially true given that, taken together, current rules on ADM appear to be fairly good at both providing individuals a right to *object* to a decision being taken automatically and to *demand explanations* (and even justification) concerning the said decision. This being said, however, does it provide them with the right to *challenge* a decision? This is something that may require further clarification at some point, and which we are now examining.

In principle, there is indeed a right to challenge decisions based on ADM. A fundamental principle of law in any jurisdiction that is based on the rule of law is the right to an effective remedy, and the right to a fair trial,[94] should the said remedy be ultimately provided by a judge. However, the costs of litigation can be high and courts already have a lot to do. It would therefore be useful for individuals to be able to request that decisions affecting them be taken by identified — and clearly accountable — human beings that cannot launder their agency, because they are given the organisational and technical capacity to override decisions reached by machines. But in practice, this is not always the case, even if it goes against the right set forth in Article 22, which means that DPAs and courts are ultimately the only solution to enforce Article 22.

The suggestion made by the Ada Lovelace Institute in its policy brief on the Data (Use and Access) Bill in the UK[95] to clarify what constitutes meaningful human intervention — and, therefore, non-automated decision making — may help clarify this point. Their proposal is to define such "human in the loop" as "a natural person with the necessary competence and authority to understand and alter the decision".[96]

Within Article 22, this could be achieved by adding a paragraph at its end that would clarify what constitutes a decision that is *not* based *solely* on ADM, even though what it states can mostly already be deduced from the GDPR. This would also make it clear that, despite the conclusions reached in some national cases,[97] Article 22 should apply even when only part of a decision was reached fully automatically. Indeed, it would not be logical for this provision to include a provision on how to handle objections to the automated nature of ADM if the existence of such a possibility meant that it would not apply. However, because it only makes explicit what is arguably already implicitly present in the current state of the law, and would make little practical difference to debatable existing national case law, this is just a slight change, which may in fact be achieved through court decisions without requiring any changes to the actual regulation.

Article 22
Automated individual decision-making, including profiling
[…]
5. When reaching a decision referred to in paragraph 1, data controllers must notify it without delay to the data subject. The decision is only valid if the data subject has been provided with a clear possibility to object to it having been reached based solely on automated processing, including profiling. This possibility must include at least the review without undue delay of the decision by a natural person with the necessary competence and authority to understand and alter the decision. The application of the decision based solely on automated processing, including profiling, is suspended until the review is completed.

Data protection by design and by default (Article 25)

Pierre Dewitte
Ensuring that data protection by design meets its objective
Gravity of the proposed changes: serious

Introduction

What motivated the EU legislator to embrace a "by design" approach to data protection in the GDPR is threefold.[98] First, its ambitions to ensure the flexibility and future-proofness of the legal framework. Instead of trying to anticipate and address *all* the *risks* raised by upcoming technologies, data protection by design strives to ensure the

[90] Case C-203/22, *CK v Dun & Bradstreet Austria GmbH and Magistrat der Stadt Wien* ECLI:EU:C:2025:117 [2025] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0203>.

[91] Case C-588/21-P, *Public.Resource.Org, Inc. and Right to Know CLG v European Commission* ECLI:EU:C:2024:201 [2024] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0588>.

[92] Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689 <http://data.europa.eu/eli/reg/2024/1689/oj>.

[93] Häuselmann, A., 'Déjà vu? An Analysis of Explanations Concerning Decision-Making Under the GDPR and the AI Act' (2025) 2(1) Journal of AI Law and Regulation 37 <https://doi.org/10.21552/aire/2025/1/6>.

[94] In Europe, this principle is laid down mainly in Article 6 ECHR and Articles 41, and Chapter VI CFR.

[95] Ada Lovelace Institute, 'Policy briefing – Data (Use and Access) Bill: Committee Stage (4 March 2025) <https://bills.parliament.uk/publications/59409/documents/6109>.

[96] Ibid., 5.

[97] Cases VG Bremen (Germany) - 2 K 763/23, [2025] <https://www.juris.de/static/infodienst/autoren/D_NJRE001618079.htm> and BVwG (Austria) - W256 2235360-1, ECLI:AT:BVWG:2025:W256.2235360.1.00 [2025] <https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20250901_W256_2235360_1_00/BVWGT_20250901_W256_2235360_1_00.html>.

[98] For a detailed overview of the history that led to the adoption of Article 25 (1), cf. Dewitte P., 'A Brief History of Data Protection by Design: From Multilateral Security to Article 25(1) GDPR' (2023) 2023 Technology and Regulation 80 <https://doi.org/10.7126/5n27g6m54>.

sustainability of a set of general *principles* designed to govern *all forms* of personal data processing.[99] Second, it aims to shift the burden of identifying and mitigating these risks onto *controllers* by articulating the Regulation around the principle of "accountability". Controllers are now given ample room for manoeuvre as to *how* to comply with their obligations as long as they are able to *demonstrate* the "appropriateness" of their choice of "technical and organisational measures". Lastly, it intends to stimulate the implementation of privacy and data protection countermeasures as early as possible in the development lifecycle. Doing so, notes the EDPB, is in controllers' best interest, as it is both "challenging and costly to make changes to plans that have already been made and [to] processing operations that have already been designed".[100] However, the manifestation of data protection by design in the GDPR suffers from several limitations that prevent it from achieving these objectives.

A paradigm shift. Broadening the personal scope of application

In its current form, data protection by design only applies to "controllers". That regulatory approach therefore assumes that the "natural or legal person that determines the purposes and the means of a given processing" is also *factually* capable of influencing the selection of the technical and organisational measures referred to in Article 25(1). Yet, controllership does not *always* coincide with meaningful influence over the design of every element of the underlying processing infrastructure, be it hardware or software.[101] As production increasingly moves towards the assembling of *existing* components developed by *third parties*, such a scenario has become the exception rather than the rule. Nowadays, most consumer-facing software services are indeed the product of complex processing operations involving multiple actors intervening at different stages of intricate supply chains. As a result, controllers often find themselves in a situation where they are legally required to implement measures that they have little to no agency over, all the while taking the blame in case such measures prove to be "inappropriate". That disconnect between the *influence* over certain design decisions and the allocation of *responsibilities* pursuant to Article 4(7) ranks high among the criticisms formulated against data protection by design,[102] as it hinders one of the main objectives of that provision, i.e., forcing technology providers to embed privacy considerations into their development lifecycle.

There are three ways around that misalignment. First, one could argue in favour of a broader interpretation of Articles 4(7) and 26 that would partially shift the burden of complying with data protection by design onto the entities that are best equipped to implement the measures referred to in Articles 25(1) — an approach that the CJEU has consistently vouched for to ensure an effective protection of the fundamental rights and freedoms of natural persons.[103] Yet, such a liberal interpretation of these provisions might drag every entity that ever contributed to the processing into a situation of joint controllership.[104] This, in turn, risks diluting the protection afforded by the Regulation to

[99] In doing so, Article 25(1) elaborates on an idea that its predecessor, the DPD, already hinted at in Article 17(1) and Recital 46 in relation to security measures.

[100] EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (20 October 2020), para. 36 <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en>.

[101] Gürses and van Hoboken expressed similar concerns when identifying "modularity" as one of the characteristics of the "agile turn", whereby "[o]rganizations of various kinds are pulled into using 'software as a service' delivered by third parties when structuring their offerings to their own end-users, thereby taking on the role of 'service curators'". As a result, they "regularly default end-users into other services and the choices these third parties make with respect to privacy governance". Cf. Gürses S., and van Hoboken J., 'Privacy after the Agile Turn' in Selinger E. et al. (eds.), *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018) 586 and 588 <https://doi.org/10.1017/9781316831960.032>.

[102] Bygrave L., 'Data Protection by Design and by Default' in Garben S. and Gormley L. (eds.), *Oxford Encyclopedia of European Union Law* (2023) 23 <https://opil.ouplaw.com/display/10.1093/law-oeeul/law-oeeul-e138>; Rubinstein I., and Good N., 'The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default' (2020) 10 International Data Privacy Law 37, 43 <https://doi.org/10.1093/idpl/ipz019>; Hildebrandt H., and Tielemans, L., 'Data Protection by Design and Technology Neutral Law' (2013) 29 Computer Law & Security Review 509, 517 <https://doi.org/10.1016/j.clsr.2013.07.004>; Klitou D., 'A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design', *Privacy Technologies and Policy* (Springer 2012) 92–93 <https://doi.org/10.1007/978-3-642-54069-1_6>; Spiekermann S., 'The Challenges of Privacy by Design' (2012) 55 Communications of the ACM 38, 38 <https://doi.org/10.1145/2209249.2209263>.

[103] Case C–604/22 *IAB Europe v Gegevensbeschermingsautoriteit* ECLI:EU:C:2024:214 [2024] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62022CJ0604> para. 55; Case C–231/22 *État belge v Autorité de protection des données* ECLI:EU:C:2024:7 [2024] <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62022CJ0231> para. 28; Case C–683/21 *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija* ECLI:EU:C:2023:949 [2023] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0683> para. 29; Case C–807/21 *Deutsche Wohnen SE v Staatsanwaltschaft Berlin* ECLI:EU:C:2023:950 [2023] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0807> para. 40; Case C–319/20 *Meta Platforms Ireland Limited, formerly Facebook Ireland Limited, v Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV* ECLI:EU:C:2022:322 [2022] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62020CJ0319> para. 73; Case C–40/17 *Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV* ECLI:EU:C:2019:629 [2019] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0040> para. 66; Case C–25/17 *Tietosuojavaltuutettu* ECLI:EU:C:2018:551 [2018] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0025> para. 66; Case C–210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388 [2018] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62016CJ0210> para. 28; Case C–131/12 *Google Spain v Agencia Española de Protección de Datos* ECLI:EU:C:2014:317 [2014] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62010CJ0360> para. 34.

[104] Rossello R., and Dewitte P., 'Exploring the Limits of Joint Control: The Case of COVID-19 Digital Proximity Tracing Solutions' (2021) 12 Journal of Intellectual Property, Information Technology and Electronic Commerce Law <https://www.jipitec.eu/jipitec/article/view/318>; Chen J. et al., 'Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 International Data Privacy Law 279 <https://doi.org/10.1093/idpl/ipaa011>; Millard C., 'At This Rate, Everyone Will Be a [Joint] Controller of Personal Data!' (2019) 9 International Data Privacy Law 217 <https://doi.org/10.1093/idpl/ipz027>; Mahieu R. et al., 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe' (2019) 10 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 85 <https://www.jipitec.eu/jipitec/article/view/247>.

data subjects.[105]

Second, one could propose that controllers try to secure a contractual commitment to abide by the letter of Article 25(1) from the *other entities* involved in the processing, regardless of their qualification. However, legal incentives to do so are rather limited. Article 26 is silent on the type of clause to be included in *joint controllership* agreements. So is Article 28 (3) when it comes to *controller-processor* agreements.[106] At best, Article 28(1) incentivises *processors* to consider the implementation of appropriate technical and organisational measures by obliging *controllers* themselves to only rely on "processors providing sufficient guarantees" to do so. Recital 78, for its part, is a mere encouragement enshrined in a non-binding provision. Yet, defaulting to contract hinges on another fiction: that of assuming that controllers and their joint controllers, processors and third parties always negotiate on equal footing. In practice, though, any form of "arrangement" is bound to suffer from both power and information asymmetries that are common where controllers heavily depend on components developed by third parties for the provision of their core services. This is especially true for smaller market players that might not always be in the driver's seat when negotiating data protection clauses with, say, advertising, authentication, cybersecurity, location, payment or storage partners — to only mention a few of the most popular ones.[107]

Third, one could try to look at other regulatory frameworks that impose a similar obligation on "producers of the products, services and applications" that is not hamstrung by the narrow personal scope of application of the GDPR. Article 3(3)e of the Radio Equipment Directive (RED) is one such avenue, as it opens up the possibility for the European Commission to mandate manufacturers of radio equipment to "incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected".[108] In 2021, the Commission seized that opportunity to extend that requirement to any "internet-connected radio equipment" that is capable of processing personal data within the meaning of the GDPR, or traffic and location data within the meaning of the ePrivacy Directive.[109] In 2022, the Commission requested harmonised standards be drafted in support of that new obligation.[110] Yet, it only became applicable in August 2025.[111] Another alternative is the Cyber Resilience Act (CRA), which shall soon require "manufacturers" of "products with digital elements" to conduct a cybersecurity impact assessment, and to ensure that such products have been designed, developed and produced in accordance with a list of "essential cybersecurity requirements".[112] Yet, and while "data minimisation" explicitly features in that list, the material scope of both the RED and the CRA revolves around narrower conception of "risk" than in the GDPR; that is, one that is primarily concerned with security, rather than with data subjects' fundamental rights and freedoms.[113] That said, the broader personal scope of application of these two frameworks goes a long way in re-aligning influence and responsibilities when it comes to ensuring appropriate security, an obligation that the GDPR only imposes on entities that qualify as either "controllers" or "processors".

None of the options detailed above is realistic (yet). Broadening the personal scope of Article 25(1) is therefore essential for data protection

[105] As noted by Advocate General Michal Bobek in its Opinion in the *Fashion ID* case, "effective protection of something tends to dramatically decrease if everyone is made responsible for it. Making everyone responsible means that no one will in fact be responsible. Or rather, the one party that should have been held responsible for a certain course of action, the one actually exercising control, is likely to hide behind all those others nominally 'co-responsible', with effective protection likely to be significantly diluted". Cf. Case C-40/17 *Fashion ID*, Opinion of Advocate General Bobek <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CC0040> para. 105.

[106] The standard contractual clauses adopted by the European Commission pursuant to Article 28(7) GDPR are equally silent on the matter. Cf. Commission Implementing Decision 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation 2018/1725 of the European Parliament and of the Council [2021] OJ L199/18 <https://data.europa.eu/eli/dec_impl/2021/915/oj>.

[107] Finck also notes that any form or arrangement, regardless of its substance or nature, "presumes that joint controllers are *aware* of their respective existence and *able* to conclude such an agreement" (emphasis added). Referring to the decision in *Wirtschaftsakademie* (n 103) and *Fashion ID* (n 103), she argues that "[i]t is an illusion to think that any genuine discussions regarding the design of responsibility could have taken place", as "[f]an page administrators [such as in *Wirtschafstakademie*, NDLR] or users of plug-ins [such as in Fashion ID, NDLR] often lack the required expertise, capital and capacity" to enter into such agreements. Cf. Finck M., 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law' (2021) 11 International Data Privacy Law 336 <https://doi.org/10.1093/idpl/ipab017>.

[108] Article 3(3)(e) of Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ L153/62 <https://data.europa.eu/eli/dir/2014/53/oj>.

[109] Article 1(2)(a) of the Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive [2022] OJ L7/6 <https://data.europa.eu/eli/reg_del/2022/30/oj>.

[110] Commission Implementing Decision C(2022)5637 of 5.8.2022 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30 [2022]. However, the document is nowhere to be found on the Commission's eNorm platform, accessible at <https://ec.europa.eu/growth/tools-databases/enorm/>.

[111] Delegated Regulation (EU) 2022/30 was scheduled to apply as of 1 August 2024, but the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC), tasked with preparing new harmonised standards in support of Article 3(3), points (d), (e) and (f) of the RED, 'have asked for an extension of the period specified in the request, for at least nine months, in order to be able to address the complex issues and problems encountered with respect to the preparation of the relevant harmonised standards and to provide harmonised standards of high quality'. See Commission Delegated Regulation (EU) 2023/2444 of 20 July 2023 amending Delegated Regulation (EU) 2022/30 as regards the date of application of the essential requirements for radio equipment and correcting that Regulation [2023] OJ L 27.10.2023 <https://data.europa.eu/eli/reg_del/2023/2444/oj>.

[112] Articles 6(a), 13(1) and (2), and Part I of Annex I, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L 20.11.2024 <https://data.europa.eu/eli/reg/2024/2847/oj>.

[113] Article 3(37) CRA (n 112) indeed defines the notion of "cybersecurity risk" as "the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident". An "incident", in turn, is conceived by reference to Article 6(6) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 27.12.2022 as an "event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data".

by design to fulfil its rationale. While one could be tempted to replace the term "controller" with "producer of products, services and applications" and leave the remainder of the provision untouched, doing so would bring its own set of issues.[114] First, it would force these actors to implement measures to ensure that the processing of personal data is performed in accordance with a set of requirements that remain only applicable to *controllers* and *processors*. While the *idea* is sound, hot swapping one concept for another without also adjusting the addressees of these obligations is bound to spark interpretation issues. Second, the temporal triggers for data protection by design to kick in — that is, the moment of the "determination of the means for processing" and that "of the processing itself" — remains intrinsically tied to the definition of "controller".

Instead, the proposed amendment follows a two-step approach. First, it extends the addressees of Article 25(1) to "processors", as suggested by the European Data Protection Supervisor (EDPS) in its Opinion on the data protection reform.[115] Second, it introduces a standalone obligation for "manufacturers" of "products" used to process personal data to ensure that these products enable controllers and processors to comply with their own obligations, as the EDPS proposed back in 2011 when commenting on the Commission's earliest reform ideas.[116] Rather than introducing new definitions that would exacerbate conceptual fragmentation, the proposed amendment takes advantage of the notions enshrined in the revised Product Liability Directive as they cover a broad range of actors and situations, including software.[117] That new obligation would open up the possibility for administrative and judicial authorities to go after all the actors involved in the development lifecycle in proportion to their respective responsibilities for the materialisation of a given risk to data subject's fundamental rights and freedoms.[118]

A pruning exercise. Rationalising the material scope of application

As it stands, Article 25(1) overlaps with other provisions of the Regulation.[119] More specifically, with Article 24(1). The former adds the "state of the art" and the "cost of implementation" to the equation, complements the latter with a timing dimension, illustrates the type of measure that controllers can implement, and slightly differ in its material scope of application. Other than that, Articles 24(1) and 25(1) share a common rationale and methodology. Besides, Article 25(1) already encapsulates the idea of data protection by default, which, in essence, is but a reaffirmation of both the necessity test that conditions the use of all the lawful grounds listed in Article 6(1) but consent, and of the purpose limitation and data minimisation principles enshrined in Article 5(1)(b) and (c).[120] Article 25(2) merely specifies the type of countermeasures that controllers must *in any case* implement as part of their obligations under Article 25(1) in situations where data subjects are offered a certain degree of agency over the processing of their personal data; as such, it is redundant, and unnecessary for Article 25(1) to function as intended. The proposed amendment therefore aims at consolidating these provisions around what makes data protection by design a standalone obligation, namely the "risk-based" approach and the timing element.[121]

[114] It is worth noting that, back in 2009 already, the Working Party on Police and Justice called for the framework that would replace the DPD to include "a provision translating the currently punctual requirements into a broader and consistent principle of privacy by design" that should be binding "for *technology designers and producers* as well as for data controllers who have to decide on the acquisition and use of ICT" (emphasis added). This later became Recital 78. Cf. WP29 and Working Party on Police and Justice, 'The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' (1 December 2009), para. 46 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf>.

[115] Albeit indirectly, by suggesting that complying with data protection by design "could be added to the list of specifications contained in Article 26(2) [now 28(3), NDLR]". Cf. Opinion of the European Data Protection Supervisor on the Data Reform Package (7 March 2012), para. 179 <https://www.edps.europa.eu/data-protection/our-work/publications/opinions/data-protection-reform-package_en>. The EDPS justified its more measured approach by invoking the "market incentive" that such obligations would "likely create" for "advisers, developers and producers of hardware and software" to consider data protection aspects when conceiving these solutions.

[116] More precisely, the EDPS proposed to add in "a separate obligation addressed to designers and manufacturers of new products and services with likely impact on data protection and privacy". Cf. Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union' (14 January 2011), para. 112 <https://www.edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_en>.

[117] Article 4(1) and (10) of Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L 2024/2853 <https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng>. The former defines "products" as "all movables, even if integrated into, or inter-connected with, another movable or an immovable", including "electricity, digital manufacturing files, raw materials and software". The latter defines "manufacturer" as "any natural or legal person who: (a) develops, manufactures or produces a product; (b) has a product designed or manufactured, or who, by putting their name, trademark or other distinguishing features on that product, presents themselves as its manufacturer; or (c) develops, manufactures or produces a product for their own use".

[118] One could also consider cementing these guarantees by supplementing the list of Article 28(3) with an obligation for controllers and processors to include a clause allocating their respective responsibilities for compliance with the broadened version of Article 25(1), and amending the liability regime of Article 82 to account for that change by introducing the possibility to claim compensation from the said "manufacturers". These, however, exceed the scope of the present contribution, and are not included as part of the revisions proposed below.

[119] For instance, Article 5(1) already obliges controllers to comply with its general principles. Articles 15 to 22, to follow-up on data subject's rights, including the right of access and to erasure. Article 32, to implement technical and organisational measures to guarantee an appropriate level of security. Article 89(1), to pseudonymise data used for archiving, research or statistical purposes. The list goes on.

[120] As pointed out by the ICO, Article 25(2) does not require controllers to resort to a "default to off" solution in situations where certain personal data are objectively necessary to achieve a specific purpose. This would run contrary to the very objective of the necessity test hinted at above. This is especially true when controllers rely on their legitimate interests. Such a reading would indeed require them to have these processing operations "objected to" by default, thereby defeating the entire purpose of Article 6(1)f GDPR. Cf. ICO, 'Data protection by design and by default' (19 May 2023) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-default/>.

[121] As pointed out by the EDPS, Article 25(1) in any case "complements the controller's responsibility laid down in Article 24" by "stressing some dimensions of [the measures'] implementation process already implicitly present in Article 24 and adding others, making them all mandatory". Cf. EDPS, 'Opinion 5/2018 – Preliminary Opinion on Privacy by Design' (31 May 2018) paras. 24 and 26, respectively <https://www.edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en>. Bygrave shares that interpretation when he underlines that "[t]he duty [i.e. Article 25(1)] builds on and elaborates the more generally formulated provisions on 'responsibility of the controller' in Article 24". Cf. Bygrave, L., 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 1 Oslo Law Review 105, 114 <https://doi.org/10.18261/issn.2387-3299-2017-02-03>.

Legal scholars have also criticised the current manifestation of data protection by design for its ambivalent *material* scope, namely the actual principles and rules that controllers must give effect to "by design".[122] If Article 24(1) obliges controllers to "ensure and be able to demonstrate that [the] processing is performed in accordance with this Regulation", Article 25(1) requires them to "implement data-protection principles, such as data minimisation, in an effective manner" and to "integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". The proposed amendment aims to reaffirm the fundamental right nature of the Regulation — and therefore of data protection by design — by clarifying that the objective controllers must pursue when implementing "appropriate measures" shall be to protect *all* data subject's fundamental rights, *including but not limited to* privacy and data protection, insofar as these are affected by the processing of their personal data.[123] Doing so requires conducting a specific type of fundamental rights impact assessment (FRIA), itself the sum of multiple assessments focusing on the impact of the processing of one's personal data on a specific fundamental right.[124] Ensuring compliance with the Regulation lays the groundwork for — but does not exhaust — such a FRIA.[125] The same reasoning therefore warrant removing any reference to "data protection" in the title of that provision in order to acknowledge the broader material scope of that obligation.

The type of measures that controllers must implement also deserves clarification. Article 25(1) specifically refers to "pseudonymisation" as *a* solution that controllers can rely on to comply with data protection by design.[126] While Recital 28 recalls that such inclusion "is not intended to preclude any other measure", it nonetheless suggests that pseudonymisation should play a prominent role in controllers' compliance exercise.[127] This defeats the flexibility and future-proofness objective pursued by the EU legislator.[128] Second, the requirement for these measures to be "technical" or "organisational" risks watering down the level of protection afforded to data subjects by putting too much emphasis on their *nature* rather than on their *objective*. The presence of these qualifiers indeed allows controllers to leverage a semantic argument to limit their responsibilities to *only* the implementation of measures that fall within the remit of what is commonly understood as being "technical" or "organisational".[129]

The parameters of the "risk-based" approach also warrant some fine-tuning. First, it is unclear whether controllers should calculate the "cost of implementation" by accounting for the total amount of resources spent on the implementation of a particular measure (i.e., the *gross* cost), or whether they should also factor in the benefits resulting from such measure (i.e., the *net* cost).[130] The latter calculation method will inevitably lower the final figure, and therefore affect the outcome of the proportionality assessment by tipping the scale in favour of a measure that might appear too expensive at first. Second, the "risks of varying likelihood and severity for rights and freedoms of natural persons" crystallises considerations that typically fall under the "nature, scope, context and purposes of the processing".[131] The former is therefore

[122] Uncertainties around what exactly must controllers comply with "by design" indeed a recurring critique in legal literature. Cf., on that point: Rubinstein and Good (n 102) 41; Waldman A., 'Data Protection by Design? A Critique of Article 25 of the GDPR' (2020) 53 Cornell International Law Journal 148-149, 153, 159 <https://heinonline.org/HOL/P?h=hein.journals/cintl53&i=169>; Bincoletto G., 'A Data Protection by Design Model for Privacy Management in Electronic Health Records' in Maurizio Naldi et al. (eds.), Privacy Technologies and Policy (Springer 2019) 168 <https://doi.org/10.1007/978-3-030-21752-5_11>; Veale M. et al., 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 13 <https://doi.org/10.1093/idpl/ipy002>; Koops B., and Leenes R., 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the "Privacy by Design" Provision in Data-Protection Law' (2014) 28 International Review of Law, Computers & Technology 161 <https://doi.org/10.1080/13600869.2013.801589>.

[123] This builds on the objective of the Regulation set out in Article 1(2) ("This Regulation protects fundamental rights and freedoms of natural persons and *in particular* their right to the protection of personal data") and Recital 4 ("[The Regulation] observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, *in particular* the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity").

[124] While privacy (PIA) and data protection (DPIA) are the usual suspects, the GDPR also strives to protect, for instance, freedom of expression (FoEIA), non-discrimination (NDIA), the right to conduct a business (RCBIA) or the right to an effective remedy a fair trial (RERIA). Or, literally, any other fundamental right affected by the processing of one's personal data ([X]IA). Cf. Dewitte P., 'The Many Shades of Impact Assessments: An Analysis of Data Protection by Design in the Case Law of National Supervisory Authorities' (2024) 2024 Technology and Regulation 226 <https://doi.org/10.71265/gt1rw770>. I refer the reader to that paper for an overview of the administrative and judicial case law dealing with Article 25(1) GDPR.

[125] This is in line with the conclusions drawn by Yeung and Bygrave in their cross-disciplinary analysis of the Regulation's architecture, in which they argue that "the risk-based approach necessitates that the data controller undertake a contextual 'fundamental rights risk assessment' in order to identify the appropriate level of stringency of the technical and organizational measures that must be adopted to guard against those risks from materializing". Cf. Yeung K., and Bygrave L., 'Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship' (2022) 16 Regulation & Governance 146-147 <https://doi.org/10.1111/rego.12401>.

[126] Article 24(2), for its parts, suggests "the implementation of appropriate data protection policies". All the other examples included in the original proposal from the Commission were dropped in the Council's version to make these provisions as flexible and future-proof as possible. Cf. Annex A of Dewitte (n 98).

[127] According to Borgesius, its presence in the final text is but a remnant of the lobbying from the AdTech industry to introduce a lighter regime for pseudonymised data. Cf. Zuiderveen Borgesius F., 'Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation' (2016) 32 Computer Law & Security Review 265-267 <https://doi.org/10.1016/j.clsr.2015.12.013>.

[128] Rubinstein and Good (n 102) 41 even consider the reference to "pseudonymisation" in the text of Article 25(1) as a "very poor choice" of example given the existence of more protective measure.

[129] Wiese Schartum already leaned toward a similar interpretation when he noted that "interpreting 'technical and organisational measures' in line with common parlance cannot be seen as an exhaustive indication of which measures may be legally required on the basis of the GDPR". Cf. Wiese Schartum D., '"Technical and Organisational Measures" – A Systematic Analysis of Required Data Protection Measures in the GDPR' in Herveg J. (ed.), Deep Diving into Data Protection, vol 2021 (1st edn, Larcier 2021) 295.

[130] The EDPS seems to have positioned itself in favour of calculating the net cost of implementation when it states that "when choosing technical and organisational measures for data protection, or assessing the measures taken by an organisation [...], the *benefits* organisations enjoy from their investments are balanced against the costs". Cf. EDPS (n 121) para. 95.

[131] This is best illustrated by the amalgam made by the EDPB when discussing the substance and impact of the 'nature' of the processing on the calculation of the administrative fine as per Article 83(2)(a) GDPR. More specifically, the Board held the following: "The *nature* of the processing [includes] the *context* in which the processing is functionally based [...] and all the characteristics of the processing. When the *nature* of processing entails higher *risks* [...] depending on the *context* of the processing and the role of the controller or processor, the supervisory authority may consider to attribute more weight to this factor" (emphasis added). Cf. EDPB, 'Guidelines 04/2022 on the Calculation of Administrative Fines under the GDPR' (24 May 2023), para. 53, point b) i <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_en>.

redundant. The proposed amendment aims at pruning Article 25(1) from unnecessary bloat, all the while underlining the pivotal role of the "risks" to "fundamental rights".

Lastly, the decision of the legislator to exclude the "time of the determination of the *purposes* for processing" from Article 25(1) is questionable. First, it suggests that the "appropriate measures" that controllers must implement only make sense once they start discussing the actual implementation of their processing operations. Second, it is also at odds with the very objective of data protection by design, which is to ensure that controllers identify and mitigate the risks raised by their processing activities *as early as possible* to avoid having to make challenging and costly changes to a system that has already been designed. Yet, decisions concerning the "purposes" of the processing can drastically influence the type of risks posed for a data subject's fundamental rights and freedoms. Since the temporal trigger of Article 25(1) does not always coincide with the moment at which the decisions shaping some of the most pressing risks are taken, this amendment proposes to extend it accordingly.

Article 4
Definitions
[…]
(9a) 'product' means product as defined in Article 4, point (1), of Directive (EU) 2024/2853;
(9b) 'manufacturer' means manufacturer as defined in Article 4, point (10) of Directive (EU) 2024/2853;
[…]

Article 24
(repealed)

Article 25
Responsibility of the controller and the processor
1. Taking into account **the risks of varying likelihood and severity for data subject's fundamental rights posed by the processing of their personal data**, the state of the art, **and** the **net** cost of implementation ~~**and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing**~~, the controller **and the processor** shall, both at the time of the determination of the **purposes or the** means for processing and at the time of the processing itself, implement appropriate ~~**technical and organisational**~~ measures~~**, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing**~~ in order to ~~**meet the requirements of this Regulation and protect the rights of data subject**~~ **mitigate the impact of that processing on their fundamental rights, including but not limited to privacy and data protection**.
2. ***(repealed)***
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in ~~**paragraphs 1 and 2 of**~~ this Article.

Article 25a
Responsibility of the product manufacturer
The manufacturer of a product used to process personal data shall design it in such a way as to ensure that the controller and the processor using that product are able to comply with their obligations pursuant to this Regulation.

Security of processing (Article 32)

Jarosław Greser

Strengthening data security in a changing threat environment

Gravity of the proposed change: moderate

Introduction

Security of personal data is key to achieving the objective of the Regulation.[132] Article 32 is meant to focus on the requirements concerning security of the processing, especially to serve as a basis for establishing liability for a breach of data, which has become one of the major challenges to security. The validity of this legislative assumption is evidenced by the statistics on fines imposed for the violation of the Regulation, which indicate that between 2018 and 2025, out of a total of 2596 violations, 418 referred to Article 32.[133] This provision has been among the most frequently cited in the case law of the CJEU.[134]

At the same time, a generally favourable assessment of the solution adopted does not preclude its further improvement. The revised wording of the provision should take into account the challenges posed by technological progress, as well as the work of researchers and jurisprudence. Furthermore, the special position of Article 32 within the overall framework of EU cybersecurity law — understood as a set of rules designed to secure the digital environment — should also be considered. The framework rests on three pillars: network security, technology security, and data security. At the time of the GDPR adoption, it was supported by a relatively narrow scope of the NIS Directive.[135] Therefore, drawing on the broad definition of personal data,[136] Article 32 became the bottom line for cybersecurity obligations in the fields of Internet of Things (IoT), cloud computing and AI. The EU's legislative activity in the area of cybersecurity has since resulted in regulating most relevant areas,[137] which has reduced the role of Article 32 in comparison with more targeted legal solutions. However, it continues to complement more specific obligations and, more importantly, plays the role of a last resort in situations where no other norms apply, such as in the case of emerging technologies, including quantum computing.

The amendment is designed to strengthen the security of data processing, thereby directly enhancing the protection afforded to data subjects. At the same time, it reduces legal ambiguity and facilitates the

[132] Bygrave L., 'Article 32' in Kuner C. et al. (eds.), *Compilation from The EU General Data Protection Regulation: A Commentary (2nd edition) Forthcoming from Oxford University Press* (Oxford University Press 2026) 59 <https://www.law.kuleuven.be/citip/en/docs/books/oup-gdpr-commentary-2nd-edition-compilation-march.pdf/view>; Case C-741/21, *GP v juris GmbH* ECLI:EU:C:2024:288 [2024] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0741> paras. 48-54.

[133] Schmid A., and Esser L., 'Numbers and Figures', *CMS law* (May 13, 2025) <https://cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures>.

[134] Daigle B., and Khan M., 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities' (2020) United States International Trade Commission Journal of International Commerce and Economics 8–9 <https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf>.

[135] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ 2016 L194/1.

[136] Purtova N., 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40 <https://doi.org/10.1080/17579961.2018.1452176>.

[137] Bygrave L., 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes' (2025) 56 Computer Law & Security Review 106071 <https://doi.org/10.1016/j.clsr.2024.106071>.

practical implementation of the Regulation by data controllers, while conforming to EU objectives to increase economic competitiveness,[138] particularly through a risk-centred approach[139] and the introduction of harmonised standards.[140]

Criteria for better assessment

The first amendment concerns removing the costs of implementation from the criteria to assess the proper choice of technical and organisational measures. The following three arguments support the proposed solution. First, the term at issue is ambiguous: it misleadingly suggests an exclusively measurable criterion. In reality, the costs of implementation must be assessed subjectively, taking into account not only the controller's current financial capacity but also their forward-looking expectations, including planned investments and prevailing market conditions. However, demonstrating such subjective costs to a supervisory authority or a court is likely to be difficult. Second, the literal wording of the provision restricts costs to those arising from implementation of organisational and technical measures, thereby excluding other relevant expenditures, such as maintenance and subsequent development of adopted solutions, which may exceed initial implementation costs.[141] Third, the provision's underlying purpose is the protection of fundamental rights and freedoms, which cannot be adequately reduced to a mere monetary calculation. Nonetheless, this protection is not absolute: its limits should be determined by principles of rational legal interpretation, notably proportionality and risk-based assessment, aimed at selecting appropriate measures to address the identified risk.

The introduction of the criterion of systemic risk as an additional lens through which the assessment of threats to the rights and freedoms of natural persons is carried out is meant to draw attention to the broader context of issues arising from data processing, particularly in AI systems. The aim is to look beyond fundamental rights and consider the wider social context, because studies show that a lack of data security can affect not only individuals but also society as a whole or specific groups within it.[142] This encompasses concerns related to the adverse effects on free speech and electoral processes, damage to law and justice, harm to media and public discourse, and negative impacts on public health, the economy and the environment.[143] Adding this criterion would not eliminate the duty to perform DPIAs under Article 35, as the objectives and the reach of these provisions differ. The amendment aims to provide additional contextual guidance for security-related assessments, whereas DPIAs target processing that is likely to result in a high risk to the rights and freedoms of natural persons. Consequently, the amendment increases the protective scope for data subjects in situations where the controller has no DPIA obligation.

Technical and organisational measures for evolving technology

With respect to the technical and organisational measures for data protection, Article 32(1) provides four protective measures as examples. At this point, the amendment introduces two changes. The first is of an editorial nature and intended to provide a clearer interpretation of the provision. This is based on a view that the obligations contained in them "do not constitute measures in the sense of intentional actions".[144]

The second amendment is substantive and may be divided into two parts. The first introduces a requirement for data encryption, unless a risk assessment concludes that this is not needed. It should be noted that an analysis of previous cases involving violation of Article 32 indicates that the absence of encryption significantly increases the harm caused in instances of unauthorised data access. Such harm could be easily mitigated through the use of encryption.[145] Moreover, encryption is regarded as a key mechanism for maintaining public trust in digital technology and the development of the digital technology sector.[146] Additionally, the introduction of this requirement serves to counter growing trends within the EU[147] aimed at lowering security standards due to vaguely defined national security issues.[148]

The second part involves the widening of the catalogue of privacy-enhancing techniques (PETs). The existing literature suggests that, in many cases, pseudonymisation does not provide an adequate level of data protection.[149] Similar concerns may be raised with respect to synthetic data[150] and data federation.[151] At the same time, the use of

[138] Draghi M., 'The Future of European Competitiveness – A Competitiveness Strategy for Europe' (2024) <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059>.

[139] Risk is inherently entangled with return and competitiveness of the entity, see: Fiegenbaum A., and Thomas H., 'Strategie Risk and Competitive Advantage: An Integrative Perspective' (2010) 1 European Management Review 84 <https://doi.org/10.1057/palgrave.emr.1500002>.

[140] On competitiveness and standardisation see: European Commission. Joint Research Centre, 'How Will Standards Facilitate New Production Systems in the Context of EU Innovation and Competitiveness in 2025?: Final Report' (Publications Office of the EU 2015) 37 <https://data.europa.eu/doi/10.2788/80985>.

[141] Lubasz D., *RODO dla AI. Zgodność z Zasadami Godnej Zaufania Sztucznej Inteligencji w Modelu Data Protection by Design* (Wolters Kluwer Polska 2025) 260; Piltz C., 'Art. 32' in Gola P. (ed), *Datenschutz-Grundverordnung: VO (EU) 2016/679: Kommentar* (CH Beck 2017) 482.

[142] Kloza D. et al., 'What Could Possibly Go Wrong?: On Risks to the Rights and Freedoms of Natural Persons in EU Data Protection Law, Their Typologies and Their Identification' (2024) 2024 Technology and Regulation 309 <https://doi.org/10.71265/148r5752>; Hinds J. et al., "It Wouldn't Happen to Me': Privacy Concerns and Perspectives Following the Cambridge Analytica Scandal' (2020) 143 International Journal of Human-Computer Studies 102498 <https://doi.org/10.1016/j.ijhcs.2020.102498>; Cruz F., 'How Antigovernment Extremists and QAnon Took over the Southern Border' (8 August 2022) <https://www.splcenter.org/resources/hatewatch/how-antigovernment-extremists-and-qanon-took-over-southern-border/>; Oyewale Oladoyinbo T., 'The Effect Of Data Information Security In Digital Voting And Electoral Processes' (2024) 26 (2) IOSR Journal of Computer Engineering 11 <https://doi.org/10.9790/0661-2602031116>.

[143] See in particular: Kloza et al. (n 142) 324.

[144] Bygrave (n 132) 71.

[145] Data Protection Commission, 'Irish Data Protection Commission Fines Meta Ireland €91 Million' (27 September 2024) <https://www.dataprotection.ie/news-media/press-releases/DPC-announces-91-million-fine-of-Meta>.

[146] Spindler G., and Schmechel P., 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 JIPITEC 163 <https://www.jipitec.eu/jipitec/article/view/177/172>.

[147] European Commission, 'Communication on ProtectEU: A European Internal Security Strategy', COM(2025) 148 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2025:148:FIN>; European Commission, 'Roadmap for Lawful and Effective Access to Data for Law Enforcement' COM(2025) 349 final <https://data.consilium.europa.eu/doc/document/ST-10806-2025-INIT/en/pdf>.

[148] Atadoga A. et al., 'A Comparative Review of Data Encryption Methods in the USA and Europe' (2024) 5 Computer Science & IT Research Journal 447 <https://doi.org/10.51594/csitrj.v5i2.815>.

[149] Mondschein C., and Monda C., 'The EU's General Data Protection Regulation (GDPR) in a Research Context' in Kubben P. et al. (eds.), *Fundamentals of Clinical Data Science* (Springer 2019) 56, 58 <http://link.springer.com/10.1007/978-3-319-99713-1>.

[150] Greser J., 'Cybersecurity Framework for Synthetic Data in Training Medical AI' (2024) 15 European Journal of Risk Regulation 903 <https://doi.org/10.1017/err.2024.74>.

[151] Wang T. et al., 'A Secure Data Collection Method Based on Spatial Data Federation', *2024 6th International Conference on Internet of Things, Automation and Artificial Intelligence (IoTAAI)* (IEEE 2024) <https://ieeexplore.ieee.org/document/10692511/>.

multiple PETs significantly enhances the level of data security,[152] and the above-mentioned solutions are frequently recommended in many cases. Listing these solutions in Article 32 would reinforce the regulatory preference, widely acknowledged in academic literature, for their use wherever feasible,[153] and therefore raising the overall standard of data processing security.

Harmonised standards to demonstrate compliance with Article 32 requirements

Another amendment concerns the inclusion of harmonised standards, publishable in the Official Journal, among the measures that may be used to demonstrate compliance with the requirements of Article 32.[154] The existing practice shows that the instruments set out in Articles 40 and 42 have not led to significant improvement in the security of data processing, due to their very limited use. For example, statistics as of February 2025 show that there were only three supranational and twenty-eight national codes of conduct[155] in effect across the EU, whereas there are only nine certification mechanisms, seals and marks registered thus far by the EDPB.[156] Furthermore, there is a noted reluctance among businesses to adopt these solutions, largely due to the disproportionate costs in relation to the benefits obtained.[157] Simultaneously, there is an entire set of standards regulating the issues of privacy and security, such as those from the ISO/IEC 27,000 family, which are widely recognised as reflecting the state of the art as set out in Article 32.[158] In the area of cybersecurity, various initiatives have also resulted in the development of European certification schemes.[159] The absence of any reference to such mechanisms in the GDPR is inconsistent with social expectations, views of the legal doctrine[160] and other EU legislative acts that permit such solutions, e.g., Article 40 AI Act. Naturally, a system based on certification has its own shortcomings,[161] which should be reformed. Therefore, the amendment limits the mechanism only to standards developed by European certification bodies based on guidelines from the Commission and subsequently undergoing the publication procedure in the Official Journal. This ensures that such standards will reflect a European approach to data protection.

The final amendment refers to the extension of the obligation imposed on the controller or the processor to legitimise the individual's processing data on their behalf. First, a requirement is introduced to ensure that any natural person acting under the authority of the controller or the processor processes data solely on their instructions, unless otherwise required by law. Second, such individuals should be properly informed and trained with respect to the applicable technical and organisational measures.[162] It should be emphasised that the inclusion of such provisions serves a clarifying function as these obligations can be inferred from the case law of the CJEU[163] and the guidelines of the EDPB.[164] Incorporating them into the text of the Regulation would highlight the responsibility of the controller or the processor in ensuring the security of data processing and in addressing the phenomenon of the illusion of control, i.e., a situation in which organisations establish formal procedures to create the appearance of control over processes, even though such procedures are not applied in practice.[165]

Article 32

Security of processing

1. Taking into account the state of the art, ~~**the costs of implementation and**~~ the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons**, including systemic risks in the Union stemming from processing data**, the controller and the processor shall implement appropriate technical and organisational measures to ensure ~~**a**~~ **the highest** level of security appropriate to the risk, including ~~**inter alia as appropriate**~~ **in particular:**

(a) ~~**the pseudonymisation and**~~ encryption of personal data;

(ab) the pseudonymisation, the processing of synthetic data or data federation;

(b) ***(repealed)***

(c) ***(repealed)***

(*continued on next page*)

[152] European Commission. Joint Research Centre., 'Technological Enablers for Privacy Preserving Data Sharing and Analysis: A Comparative Study' (Publications Office 2023) <https://data.europa.eu/doi/10.2760/427718>.

[153] Papadaki E., and Stalla-Bourdillon S., 'Art. 32' in in Spiecker et al. (eds.), *General Data Protection Regulation* (1st edn, Nomos Beck Hart 2023) 659.

[154] "A 'harmonised standard' means a non-binding technical specification adopted by a standardisation body, namely the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) or the European Telecommunications Standards Institute (ETSI), on the basis of a remit issued by the Commission" Cf. Article 2 (l) Directive 2006/42/EC on machinery, and amending Directive 95/16/EC (recast) [2006] OJ 2006 L157/24 <http://data.europa.eu/eli/dir/2006/42/oj>; Kamara I., 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation 'Mandate'' (2017) 8 European Journal of Law and Technology <https://ejlt.org/index.php/ejlt/article/view/545/723>.

[155] Selbstregulierung Informationswirtschaft e.V., 'Codes of Conduct under GDPR Overview on Benefits and Impacts of Codes of Conduct alongside a List of Current Codes of Conduct' (2025) <https://sriw.de/fileadmin/sriw/files/202502_European_Codes_of_Conduct_under_GDPR_v0-9.pdf>.

[156] EDPB, 'Register of Certification Mechanisms, Seals and Marks' <https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en>.

[157] Kamara I. et al., 'The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act' (2020) 8–9 <https://repository.tilburguniversity.edu/server/api/core/bitstreams/dbea6af9-dca9-4aef-b83a-2d5535b7ffb0/content>.

[158] Prezes Urzędu Ochrony Danych Osobowych, Decyzja DKN.5130.2215.2020 <https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020>.

[159] Kohler C., 'The EU Cybersecurity Act and European Standards: An Introduction to the Role of European Standardization' (2020) 1 International Cybersecurity Law Review 7 <https://doi.org/10.1365/s43439-020-00008-1>; Khurshid A. et al., 'EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme' (2022) 10 IEEE Access 129932.

[160] Kamara (n 154).

[161] Du Boispéan S. et al., 'Introduction to the European New Legislative Framework' in Mueck M. and Gaie C. (eds), *European Digital Regulations*, vol 265 (Springer 2025) <https://link.springer.com/10.1007/978-3-031-80809-8_1>; Volpato A., and Eliantonio M., 'The Participation of Civil Society in ETSI from the Perspective of Throughput Legitimacy' (2024) 37 Innovation: The European Journal of Social Science Research 1375 <https://doi.org/10.1080/13511610.2024.2321852>.

[162] Human competencies are crutial to fulfill GDPR requirements, requiring different competencies depending on sector and responabilities, see for example: Kamenjasevic E., and Fabcic Povse D., 'A Data Protection Perspective on Training in the mHealth Sector' in Andreoni G. et al. (eds.), *m_Health Current and Future Applications* (Springer 2019) 2 <http://link.springer.com/10.1007/978-3-030-02182-5_5>.

[163] Case C-741/21, *GP v juris GmbH* (n 132) para. 49; Case C-687, *BL v MediaMarktSaturn Hagen-Iserlohn GmbH* ECLI:EU:C:2024:72 [2024] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0687> para. 38; Case C-340/21, *VB v Natsionalna agentsia za prihodite* ECLI:EU:C:2023:986 [2023] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0340> paras. 30–32.

[164] EDPB, 'Guidelines 01/2021 on Examples Regarding Personal Data Breach Notification' (Version 2.0) 7 <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en>.

[165] Slapničar S. et al., 'Cyber Risk Management: An Illusion of a Risk-Based Approach' (2024) SSRN <https://www.ssrn.com/abstract=4949619>.

(*continued*)

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1a. In light of the premises set forth in paragraph 1, the controller and the processor shall implement technical and organizational measures to achieve the appropriate capability to:

(a) ensure confidentiality, integrity, availability, and resilience of processing systems and services; and

(b) restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

2. In assessing the appropriate level of security account shall be taken in particular of the risks **and systemic risks** that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 ~~**or,**~~ an approved certification mechanism as referred to in Article 42 **or harmonised standards which have been published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012*** may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

3a. In accordance with Article 10 of Regulation (EU) No 1025/2012, the Commission may issue standardisation requests concerning the requirements for technical and organisational measures as set out in paragraph 1 of this Article.

4. The controller and processor shall ~~**take steps to**~~ ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law**, and such natural person shall be informed and continuously trained on technical and organisational measures that the controller or the processor have adopted.**

—

* OJ L 316, 14.11.2012, p. 12–33.

Data protection impact assessment and prior consultation (Articles 35–36)

Dariusz Kloza

Improving legal certainty and facilitating a meaningful (serious, useful, etc.) DPIA

Gravity of the proposed change: moderate

Introduction

The process of data protection impact assessment (DPIA) brings many benefits for data controllers and data subjects alike.[166] If taken seriously — to the former — it rationalises the decision-making process, demonstrates due diligence and accountability, and — to the latter — it contributes to a higher level of protection of personal data.[167] Overall, the inclusion of a requirement to carry out a DPIA in EU data protection law is a welcome development.

With critics already seeing the DPIA requirement under the GDPR as a heavy burden, its functioning has furthermore demonstrated several difficulties. These range from the very understanding of basic concepts on which it has been construed (e.g., "risk to the rights and freedoms of natural persons") to a litany of practical difficulties, as illustrated by one viral, memorable meme of "draw the rest of the d*** owl". Some typical problems include attempting to carry out a DPIA without first providing a systematic description of the processing operations; insufficient or incorrect risk identification; undertaking either the necessity or proportionality assessment, but not both; unclear criteria for determining the likelihood (probability) and severity of risks; lack of or inadequate explanation regarding how a specific risk level is determined; focusing on security risks and not reflecting risks to the rights and freedoms; mismatches between mitigation measures and identified risks; omission of public consultations or otherwise faulty assessment.[168]

Consistent with the foregoing, the objective of reforming the DPIA requirement is at least fourfold, namely:

1) to enhance legal certainty by: (i) offering greater clarity as to when it must be conducted and when an exemption applies, as well as (ii) further clarifying the steps necessary to carry it out;
2) to minimise fragmentation and — as a result — ensure greater harmonisation, e.g., to avoid situations where a DPIA is required in one Member State but not in another,[169] or where a Member State unilaterally requires a DPIA for certain types of processing operations ("gold-plating");
3) to work towards a DPIA bearing fruit by: (i) defining a set of quality criteria that the controller and/or its assessor, if engaged, must strive to meet to the best of their abilities, and (ii) ensuring that the scope of the DPIA requirement is future-proof, so that it continues to adequately reflect the challenges that developments of technology, economy and society bring to the fore; and
4) to offer authoritative, meaningful support to controller and assessor in carrying out a DPIA as the need for greater support from public authorities in this area has been widely acknowledged.[170]

The amendment retains the original "legal hook" approach, in which – in the interest of flexibility – only the core elements of the DPIA requirement are defined in a legal statute, which is supplemented by guidelines, standardisation, co-regulation, self-regulation etc.[171] However, the experience has shown that several additional elements must be set forth in the law, e.g., the definition of risk or the exact contents of a DPIA. That impact assessment procedures are constantly being refined is not uncommon, e.g., not only environmental impact assessment (EIA) has been governed by a standalone directive from 1985, but also it was

[166] For a general introduction, cf. e.g., Kloza D. et al., 'The Concept of Impact Assessment' in Burgess JP., and Kloza D. (eds.), *Border Control and New Technologies* (Academic & Scientific Publishers 2021) <https://doi.org/10.5281/zenodo.5121680>.

[167] For the list of benefits and drawbacks, cf. e.g., D'hulst T., and Kloza D., 'Data Protection Impact Assessment: More than Just a Compliance Tool' (Van Bael & Bellis 2022) <https://www.vbb.com/media/Insights_Articles/VBB_QA_DPIA_2022_final.pdf>; Kloza et al. (n 142) 34-36.

[168] This litany of practical difficulties is largely based on two EDPS surveys on the use of DPIAs by EU institutions, bodies, offices and agencies under Regulation 2018/1725 (in 2020: <https://www.edps.europa.eu/sites/default/files/publication/20-07-06_edps_dpias_survey_en.pdf> and 2024: <https://www.edps.europa.eu/system/files/2025-09/2025-09-08_dpia_survey_report_en.pdf), which are *per analogiam* useful for the GDPR. Furthermore, a – thus far – handful of academic papers has critically evaluated the DPIA requirement, e.g.,: Schermer BW., 'Assessing the Impact of Impact Assessments: Practical Questions Related to Article 35 of the GDPR', in Costello RA., and Leiser M. (eds.) *Critical Reflections on the EU's Data Protection Regime* (Hart 2024) 29-46 <https://doi.org/10.5040/9781509977871.ch-002>; Kloza et al. (n 142) as well as a pre-GDPR take: Kloza D. et al., 'Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies' in: Skopik F., and Smith P. (eds.), *Smart Grid Security* (Elsevier 2015) 11-47 <https://doi.org/10.1016/B978-0-12-802122-4.00002-X>.

[169] As it is currently possible with national black- and white-lists (Article 35(4)-(6)).

[170] Cf. e.g., De Hert P. et al., 'Recommendations for a Privacy Impact Assessment Framework for the European Union' (VUB 2012) Deliverable D3 of the PIAF [A Privacy Impact Assessment Framework for data protection and privacy rights] project <https://doi.org/10.5281/zenodo.5141741>; Kloza D. et al., 'Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals' (VUB 2017) d.pia.lab Policy Brief 1/2017 <https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf>.

[171] Boulanger MH., 'The data protection reform and the DPIA framework, presentation at the conference "Implementation of the RFID Privacy Impact Assessment (PIA) framework. Towards a coherent European Approach', Brussels, 8 February 2012. Cf. slide No 18.

amended already three times, codified in 2011 and most recently amended, for the fourth time, in 2014.[172]

Scope

Paragraphs 1, and 3 to 6 spell out the scope of the DPIA requirement, i.e., when a controller must carry out a DPIA, a point which the amendment further clarifies. A misleading reference suggesting the focus on new technologies as a trigger of a DPIA is removed as highly risky processing operations can equally take place when personal data are processed using some already "old" technologies such as biometrics. Instead, while the processing of personal data of any vulnerable people on a large scale is likely to pose a high risk (and hence trigger a DPIA pursuant to Article 35(1)), for the avoidance of doubt, the processing of children's personal data on a large scale is explicitly added to trigger a DPIA.[173]

Importantly, due to notorious confusion about what "risk" is, and similarly to the Network and Information Security II (NIS2) Directive,[174] the DSA[175] or the AI Act[176] — all enacted after the GDPR — a definition thereof is offered in Article 4, which refers to its common understanding (i.e., a combination of the likelihood and severity of a negative consequence).[177] This amendment aims to help assess it and distinguish risks to the rights and freedoms from other types thereof, e.g., information security risks (i.e., chances of breaching — depending on a conceptualisation — confidentiality, integrity or availability of data) or non-compliance risks (i.e., chances that a given processing operation will not comply with the law).

To enhance legal certainty, the amendment also lists situations where a DPIA is not required: first, when it would be repetitive and thus yield no new knowledge. Second, in the new paragraph 1a, when another, suitable and comparable type of impact assessment — such as various forms of regulatory impact assessment (RIA) or a FRIA under the AI Act[178] — has already, in essence, covered a DPIA under the GDPR. Consequently, paragraph 10 — narrower in scope — is repealed, thereby removing — in the interest of harmonisation — the possibility for Member States to introduce an additional DPIA requirement. Third, a DPIA is not required when a legal or medical practitioner processes personal data of its clients or patients; this codifies the already existing exemption from Recital 90, as recitals are non-binding.

Importantly, in paragraph 4, the amendment removes the national "white-" and "black-lists" expanding and shrinking, within the consistency mechanism, the scope of the DPIA requirement. The amendment replaces these lists with the obligation of the EDPB to establish and periodically review the scope of the DPIA requirement with a view to adequately reflect the challenges arising from developments in technology, economy and society. The relevant EDPB decision can be appealed to the CJEU under Article 263 of the Treaty on the Functioning of the European Union (TFEU).[179] Consequently, paragraphs 5 and 6 are repealed.

While the GDPR is, in principle, a full harmonisation instrument, Member States may "lay down additional, stricter or derogating national rules, which leave them a margin of discretion as to the manner in which those provisions may be implemented".[180] However, such "opening clauses" should not be interpreted as permitting to unilaterally require measures as far reaching as an additional DPIA requirement, as e.g., Belgium did for some processing activities for purposes of research (Article 89).[181] Therefore, the EDPB is now exclusively competent to expand or contract the scope of a DPIA requirement (paragraph 4).

Paragraph 11 — originally dealing with the need to periodically check if the processing operations comply with the results a DPIA — is repealed. Given the advisory nature of a DPIA, the GDPR impose no clear duty to mitigate the risk assessed *within this process*.[182] Both Recital 84 ("the outcome … should be taken into account when determining the appropriate measures") read together with Article 25 ("…at the time of the determination and … the processing itself") require only that DPIA *results* are considered. Instead, in the interest of the continuity of the appropriate level of protection, the new paragraph 12 introduces an obligation for the controller to review its DPIA(s) each time the risk and/or the context (e.g., technology, society or economy) change.

Contents of a DPIA

Paragraph 7, read together with paragraphs 2 and 8 (both unchanged) as well as 9, stipulate the required contents of a DPIA. Inspired by the rules on risk assessment found, e.g., in the DSA[183] or the Online Safety Act 2023 in the UK,[184] the amendment introduces a set of quality criteria for a DPIA. Namely, it must be based on relevant information and evidence, and it must be suitable and sufficient. The latter criterion means that a DPIA must include all the elements listed in Article 35, be specific to the processing operations in question, and accurately reflect the impacts.[185] These are targets which controllers and/or assessors must strive to meet, as a DPIA is an obligation of means (due diligence) and not an obligation of result. Eventually, the amendment clarifies that a process of DPIA results in a report, kept on file (cf. Article 30), to demonstrate accountability in case of an audit, investigation, complaint or claim.

In addition, while the amendment maintains that stakeholder consultation occurs when the controller deems it appropriate (paragraph 9), the lack of such consultation must be now justified. To avoid

[172] Directive 2011/92/EU on the assessment of the effects of certain public and private projects on the environment [2012] OJ 2012 L26/1 <http://data.europa.eu/eli/dir/2011/92/oj>.

[173] Alternatively, the processing of personal data concerning vulnerable people could trigger a DPIA, provided an appropriate definition of such broad category is provided. Cf. e.g., Malgieri G., *Vulnerability and Data Protection Law* (Oxford University Press 2023) <https://doi.org/10.1093/oso/9780192870339.001.0001>.

[174] Article 6(9).

[175] Article 34(1).

[176] Article 3(2).

[177] Cf. e.g., ISO 31000:2018. Cf. also Kloza et al. (n 142) 309-329.

[178] Artificial Intelligence Act (n 92).

[179] Alternatively, it is the European Commission that could be establishing and reviewing such list in a comitology procedure. Cf. Regulation 182/2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers [2011] OJ 2011 L55/13 <http://data.europa.eu/eli/reg/2011/182/oj>.

[180] Case C-319/20, *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* (n 103) para. 57.

[181] E.g., Article 191(3), Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Moniteur belge* No. 209, p. 68616.

[182] Quelle C., 'The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too' in Leenes R. et al (eds.) *Data Protection and Privacy: The Age of Intelligent Machines* (Hart 2017) 50 <http://ssrn.com/abstract=3000382>.

[183] Cf. Article 34(1).

[184] Cf. Sections 9, 11, 26 and 35 <https://www.legislation.gov.uk/ukpga/2023/50/contents>.

[185] Cf. p. 6 <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/risk-assessment-guidance-and-risk-profiles.pdf>.

prescriptiveness, reasons therefor are not stipulated by law, but typically they are meant to include situations when no promising new insights are to be gained, an advice of a data protection officer (DPO) has proven sufficient, such consultations were to breach confidentiality or the processing were urgent.[186]

The amendment further clarifies the contents of the proportionality assessment. As the protection of personal data has been since 2009 elevated in the EU to the status of a fundamental right, it now mandates the evaluation of processing operations against the five criteria for the limitation of fundamental rights, as stipulated in Article 52(1) CFR, i.e., legality, respect for the essence of the right, legitimacy, necessity and proportionality *sensu stricto*.[187]

It also rectifies a probable error where the risks should relate more broadly to the concerned natural persons and not only data subjects (as other stakeholders might face negative consequences too),[188] in line with the wording of the first sentence of Article 35(1).

Authoritative and meaningful support from DPAs[189]

Ideally, DPIAs should be easy to use and resources dedicated thereto should be spent efficiently. Both these goals are highly dependent on authoritative, meaningful support from DPAs. But the EDPB has thus far failed to update the minimalistic, theoretical guidelines that the former WP29 had issued and that the EDPB endorsed in 2017.[190] Furthermore, national DPAs often issue their own guidance material (including templates or even software), which — while reflecting national context — often do not converge.[191] In addition, guidance and templates originating from the private sector and academia differ significantly in their applicability and – needless to say – quality.

As a result, new paragraphs 13 and 14 require the EDPB to become a "reference centre" facilitating the DPIA process for controllers and assessors. First, inspired by analogous provisions, e.g., in the AI Act,[192] the EDPB is now explicitly tasked with issuing and keeping up-to-date guidelines and — especially — templates for a DPIA, subject to public consultation.[193] (Ideally, these should be informed by a critical evaluation of the support material thus far.) These materials should include also a systematic inventory of risks and a counterpart inventory of measures (controls) to appropriately address them as well as guidelines on stakeholder participation. Being a "reference centre" could also include — resources permitting — offering regular trainings with Questions and Answers (Q&A) sessions or even running a hotline explaining the DPIA requirement (but not providing any advice in individual matters).[194]

Templates should focus on the *process* rather than on *documenting* the outcome of the process. There might be a single template or several ones; if the latter — each one would be addressing specificities of a given sector (e.g., public or private), technology (e.g., biometrics or AI) or economic activity. These templates should be sufficiently detailed, and make clear what is required by the law and what is optional (e.g., best practice). They should be available in an editable format (e.g., DOCX and/or ODT). However, since they are meant to fit a variety of contexts, neither these guidelines nor these templates are binding and hence might be adjusted accordingly.

Second, the EDPB must establish and maintain a public, freely accessible and free-of-charge digital registry of DPIAs carried out throughout the European Economic Area (EEA), which controllers must populate. Controllers must register the mere fact of concluding a DPIA and provide basic yet meaningful information thereon in a non-confidential summary. Not only transparency is served, but also controllers and assessors can learn from the experience of others, showcasing best practice. The registry is modelled on its equivalent under the National Environmental Policy Act (NEPA) of 1969 in the US, i.e., the Environmental Impact Statement (EIS) Database.[195]

To prevent dependence on resources that have yet to be developed — a common issue with new legislation — the EDPB must ensure these are prepared "without undue delay" and certainly before the reformed substantive provisions start to apply.

Prior consultation

Concerning prior consultation in individual matters (Article 36(1)-(2)), the most important amendment goes beyond the mere "free advice" advantage and confers the benefits of an official, individual interpretation of the law from a public authority, as known e.g., from tax law in some jurisdictions, e.g., Poland. The opinion (written advice) binds a DPA *ad casum*, but the controller is not obliged to follow it. As a result, the controller is protected from suffering negative consequences should it turn out that this DPA, at a later stage, takes a different position to the one expressed earlier. This amendment will encourage controllers to seek such opinions, thereby enhancing the protection of personal data by likely preventing many potential infringements.

If the matter submitted for prior consultation is of general application or produces effects in several Member States, the DPA might ask the EDPB for their opinion in accordance with the procedure set forth in Article 64(2)-(3); the EDPB opinion binds the referring DPA and is challengeable under Article 263 TFEU.

To facilitate the consultation process, paragraph 3 (the contents of a request) is repealed as too prescriptive. Instead, the new paragraph 2a mandates the EDPB to provide and keep up-to-date — in addition to the relevant non-binding guidelines — a single, pan-European template for a request of prior consultation, the use of which is mandatory (this contrasts with the DPIA template(s), voluntary in nature). To further simplify the prior consultation process, a single deadline of three months now binds a DPA. Eventually, an urgent need for a prior consultation is recognised, and a failure of a DPA to act can be contested.

The amendment to paragraph 4 clarifies the scope of the prior legislative consultation. It replaces the unclear wording by aligning it with the text of Article 42(1) of Regulation 2018/1725. Paragraph 5 — dealing with a possibility for Member States to introduce prior authorisation — is

[186] Cf. <https://www.linkedin.com/posts/dkloza_dpia-gdpr-activity-7254488800867815424-fdyh>. Alternatively, stakeholder participation can be made an enforceable right, whereby the unjustified lack thereof can be actionable in a court. Cf. Kloza D., 'Public Voice in Privacy Governance: Lessons from Environmental Democracy' in Schweighofer E. et al. (eds.) *KnowRight 2012: Knowledge Rights – Legal, Societal and Related Technological Aspects* (Österreichische Computer Gesellschaft 2013) 119-144 <https://doi.org/10.5281/zenodo.6992200>.

[187] Cf. e.g., Case C-465/00, *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk* ECLI:EU:C:2003:294 [2003] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62000CJ0465> para. 86; cf. also the appendix to Bomhoff J., 'Making Legal Knowledge Work: Practising Proportionality in the German Repetitorium' (2022) Social & Legal Studies <https://doi.org/10.1177/09646639221092962>.

[188] Cf. Kloza et al. (n 142) section 3.1.

[189] Some of these measures could be adopted by the EDPB at its own initiative, pursuant to Article 70(1)(e), without the need for new legislation.

[190] WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (WP248, 4 October 2017) <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711>.

[191] E.g., the relevant guidance from e.g., the French DPA (<https://www.cnil.fr/fr/gerer-les-risques>) differs significantly from e.g., the Spanish DPA (<https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>).

[192] E.g., Article 27(5).

[193] Article 70(4).

[194] Cf. Jasmontaite L. et al., *Guidance for Data Protection Authorities (DPAs) on running a hotline dedicated to Small and Medium-sized enterprises (SMEs)* (VUB 2020) <https://brusselsprivacyhub.eu/onewebmedia/StarII-DPA%20guidance.pdf>.

[195] Cf. <https://cdxapps.epa.gov/cdx-enepa-II/public/action/eis/search>.

repealed in the interest of harmonisation.

Article 4
Definitions
[…]
(28) 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm;

Article 35
Data protection impact assessment
1. Where a type of processing ~~**in particular using new technologies, and**~~, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar**, including repetitive,** processing operations that present similar high risks.

1a. The controller is not required to carry out a data protection impact assessment if:

(a) a comparable process has already met the requirements outlined in this article; or

(b) the processing is carried out by an individual physician, other healthcare professional or lawyer in relation to their patients or clients.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; ~~**or**~~
(c) a systematic monitoring of a publicly accessible area on a large scale~~.~~**; or**

(d) processing on a large scale of personal data concerning children.

4. The Board referred to in Article 68**, with a view to adequately reflect the challenges stemming from technological, economic and social developments, has an exclusive competence to determine:**

(a) additional kinds of processing operations for which a data protection impact assessment is required;

(b) kinds of processing operations for which no data protection impact assessment is required.

5. **(*repealed*)**
6. **(*repealed*)**
7. The assessment **results in a report. The assessment shall be based on evidence, be suitable and sufficient, and** shall contain at least:
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the ~~**necessity and**~~ proportionality of the processing operations in relation to the purposes**, according to the criteria stipulated in Article 52(1) of the Charter of Fundamental Rights of the European Union;***
(c) an assessment of the risks to the rights and freedoms of ~~**data subjects**~~ **natural persons** referred to in paragraph 1; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.
9. Where appropriate, the controller shall seek the views of **concerned natural persons** ~~**data subjects**~~ or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. **The lack of such consultation must be justified.**

10. (*repealed*)
11. (*repealed*)

12. The controller shall review a carried-out data protection impact assessment each time there is a change of the risk represented by the processing or the nature, scope, context and purposes of the processing.

13. The Board shall, without undue delay, provide and keep up-to-date guidelines and templates regarding the obligations laid down in this article. The use of such templates is voluntary.

14. Upon completion of a data protection impact assessment, the controller shall, without undue delay, register a report therefrom and a non-confidential summary thereof in a freely accessible, public electronic registry maintained by the Board, the use of which shall be free of charge.

(*continued on next column*)

(*continued*)

Article 36
Prior consultation
1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to ~~**eight weeks**~~ **three months** of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. **[*Sentence repealed.*]** Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation. **In urgent situations, or if otherwise appropriate, the supervisory authority shall shorten the deadline. If the supervisory authority fails to act, Article 78(1) applies *mutatis mutandis*.**

2a. The Board shall, without undue delay, provide and keep up-to-date guidelines and a template regarding the obligations laid down in this article. The use of this template is mandatory.

2b. The written advice is binding on the supervisory authority and, to the extent it has followed it, the controller shall not bear any negative consequences should the supervisory authority subsequently adopt a different position from the one expressed in the written advice. Articles 64(2)-(3) apply *mutatis mutandis*.

3. (*repealed*)
4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, ~~**which relates to processing**~~ **where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.**

5. (*repealed*)

—

* OJ C 202, 7.6.2016, p. 389.

Derogations for specific situations (Article 49)

Laura Drechsler

Ensuring that protection travels with the data
Gravity of the proposed change: light

Introduction

The regulation of international personal data transfers in Chapter V has been a topic of much discussion,[196] even under the GDPR's predecessor — the DPD.[197] Critics of the GDPR's approach point towards its complexity, potential protectionist undertones and conflicts with

[196] Cf. e.g., Chander A., and Schwartz P., 'Privacy and/or Trade' (2023) 90(1) The University of Chicago Law Review 49 <https://chicagounbound.uchicago.edu/uclrev/vol90/iss1/2>; Yakovleva S., *Governing Cross-Border Data Flows: Reconciling EU Data Protection and International Trade Law* (OUP 2024) <https://doi.org/10.1093/oso/9780192899248.001.0001>; Kuner C., 'International data transfers and the EDPS: current accomplishments and future challenges', in *Two decades of personal data protection. What next? EDPS 20th Anniversary* (2024) 80-91 <https://www.edps.europa.eu/system/files/2024-06/edps_20thanniversary-book_en.pdf>.

[197] Directive 95/46/EC (n 36). Cf. WP29, 'Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (WP12, 24 July 1998); Kuner C., *Transborder Data Flows and Data Privacy Law* (OUP 2013) <https://doi.org/10.1093/acprof:oso/9780199674619.001.0001>.

international trade law.[198] Proponents[199] and the CJEU,[200] however, emphasize the crucial role Chapter V plays for the protection of fundamental rights of individuals whenever their personal data crosses international borders. In the words of the European Commission, "protection travels with the data".[201] Without rules on transfers, the EU's framework for personal data processing would be easily undermined by moving processing operations abroad.[202]

To achieve an EU-level of protection of fundamental rights even when data are on the move, Chapter V operates based on two principles, both of which are relevant for the amendment.

First, a transfer of personal data must never undermine the level of protection of fundamental rights of individuals granted by the GDPR. This is explicitly stated in Article 44. What constitutes a transfer is not defined in the GDPR itself. The EDPB and recent case law consider a processing operation as a transfer if a controller or processor in the scope of the GDPR (data exporter) make the data available to a controller or processor outside of the EEA (data importer).[203] The required level of protection is also defined by CJEU case law — i.e., it must be "essentially equivalent" to that enjoyed within the EEA.[204] This can be best understood as a requirement for exporters to verify whether the transfers they are undertaking interfere disproportionately with the fundamental rights of the individuals concerned.[205] An interference with the fundamental right to personal data protection is — following the case law of the Court — already reached when personal data are processed in any manner, i.e., no concrete harm on an individual level is required.[206] The crux of the assessment will therefore be on whether such an interference meets the requirements for a fundamental rights interference of the CFR, in particular whether the interference is necessary and proportionate.[207] Next to personal data protection, the CJEU has noted the fundamental rights of privacy, non-discrimination and effective judicial protection as those rights that might be interfered with by a transfer of personal data.[208]

Second, a transfer requires an (additional) "legal" basis. There are three options which operate in a sequence. Adequacy decision — i.e., assessments on essential equivalence made by the Commission — come first and should be used if adopted for the jurisdiction of the data importer.[209] Appropriate safeguards — i.e., different legal instruments listed in the law — are the second option and mandate the exporter to verify the actual level of protection achieved and to supplement if needed.[210] Finally, if neither adequacy nor appropriate safeguards are available, exporters can rely on a list of derogations — i.e., specified exceptions listed in Article 49.

This provision is difficult to untangle — paragraph 1 lists seven different derogations (i.e., explicit consent, a contract between controller and data subject, a contract in the interest of the data subject, important public interests, legal claims, vital interests of the data subject, transfers from public registers) but also includes a hidden subparagraph with no numbering presumably adding an eight option (i.e., compelling legitimate interest).[211] Paragraphs 2, 3, 4 and 6 further limit the exceptions provided, while paragraph 5 grants Member States the power limit for certain categories of data transfers for "important reasons of public interest".

Derogations and essential equivalence

It is not clear how derogations relate to the first condition for data transfers — namely that a transfer must never undermine the level of protection of natural persons. At a first glance, naming it "derogations" suggests that Article 49 presents an exception to Article 44. Consequently, exporters would not have to care about maintaining an essentially equivalent level of protection when using derogations.[212] Yet, the *Schrems II* judgment proposes a different reading. As the judgment highlights, Article 44 is an overarching principle for all of Chapter V.[213] This could mean that it also applies to derogations. To add to the confusion, the CJEU has in the same judgment, when answering the question on a potential interim period where exporters could still rely on the Privacy Shield (i.e., the adequacy decision annulled in *Schrems II*), underlined that this is not needed as derogations could be used.[214] This contrasts with the opinion of the EDPB on derogations, which concludes that due to their exceptional nature they may only be used for occasional non-recurring transfers.[215] The transfers at stake in *Schrems II* were not occasional, suggesting that this is not a limit the CJEU is posing. Recital 111 advises that the limit of occasional transfers exists for some of the derogations noted in Article 49, but not for all.[216]

Putting all the sources together reveals a conflict between the text of the GDPR, the interpretation of the EDPB and the case law of the CJEU. Consequently, there is lack of legal certainty on when and how to use derogations. This, in turn, affects their role as a fallback option, when neither adequacy decision nor appropriate safeguards are available. A situation that occurs, for example, in international research projects with partners from all over the world, where not all countries enjoy

[198] CF. e.g., Chander and Schwartz (n 196); Yakovleva (n 196).

[199] Cf. e.g., Drechsler L., and Kamara I., 'Essential equivalence as a benchmark for international data transfers after Schrems II', Kosta E., and Leenes R. (eds.), *Research Handbook on EU data protection law* (Edward Elgar 2022) 314-352 <https://doi.org/10.4337/9781800371682.00022>; Kuner (n 196) 80-91.

[200] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 [2015] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362>; *Opinion 1/15* ECLI:EU:C:2017:592 [2017] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62015CV0001(01)>; Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ECLI:EU:C:2020:559 [2020] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311>.

[201] European Commission, 'Communication: A European strategy for data', COM(2020) 66 final (19 February 2020) 23 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066>.

[202] EDPB, 'Recommendations 02/2020 on the European Essential Guarantees for surveillance measures' (10 November 2020) <https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en>; EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (Version 2.0, 18 June 2021) <https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en>.

[203] EDPB, 'Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR' (Version 2.0, 14 February 2023) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en>; Case T-354/22, *Thomas Bindl v European Commission* ECLI:EU:T:2025:4 [2025] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62022TJ0354> para. 95.

[204] Case C-362/14, *Schrems I* (n 200): *Opinion 1/15* (n 200); Case C-311/18, *Schrems II* (n 200).

[205] Article 44. Cf. Drechsler and Kamara (n 199); EDPB Recommendations 02/2020 (n 202); EDPB Recommendations 01/2020 (n 202).

[206] Cf. Case C-311/18, *Schrems II* (n 200), para. 170.

[207] Article 52(1) CFR. Drechsler and Kamara (n 199).

[208] Case C-362/14, *Schrems I* (n 200): *Opinion 1/15* (n 200); Case C-311/18, *Schrems II* (n 200).

[209] Article 45.

[210] Articles 46–47; EDPB Recommendations 01/2020 (n 202).

[211] Article 49(1).

[212] Cf. e.g., Yakovleva (n 196).

[213] Case C-311/18, *Schrems II* (n 200) para 92.

[214] Ibid., para. 202.

[215] EDPB, 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679' (25 May 2018) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation>.

[216] Cf. further Recital 112.

adequacy, and some research institutions are — due to their legal framework — not permitted to conclude the contracts required for appropriate safeguards.[217]

Two types of derogations

The amendment of Article 49 aims to clear up the legal contradiction in a manner that ensures the first principle of data transfers (i.e., protection is not undermined) is kept for all the provisions of Chapter V (following the interpretation of the CJEU), while also ensuring that derogations are not restricted when fundamental rights can be safeguarded. This helps a better application of the second principle as it makes derogation a more usable option.

To this end, the amendment splits the existing derogations into two types (see, for an overview, the table below). The first type are derogations where the law presumes that their use will not undermine the level of protection of fundamental rights of individuals. Such a presumption is based on the fact that their use is occasional and non-repetitive in specific situations listed by the law that appear justifiable in light of the criteria for a fundamental rights justification of the CFR. This presumption can be revoked, whereby the burden of proof is on the data subject provided the exporters has followed the transparency requirements with regards to transfers and the data subject is therefore aware of them.[218] From the existing derogations, the amendment qualifies the derogations for contracts, legal claims, vital interests of the data subject, transfers from public register, and for compelling legitimate interests as type 1.

The second type are those derogations where there is no assumption of essential equivalence, meaning that it is up to the exporter to demonstrate that the transfer(s) in question are not interfering with an individual's fundamental rights, similar to the duties data exporters have for appropriate safeguards. The difference between appropriate safeguards and derogations for type 2 is that the derogations are provided by the text of the GDPR, whereas appropriate safeguards include a number of different instruments such as Standard Contractual Clauses (SCC) or Binding Corporate Rules (BCR) which require some setting up on the side of the data exporters. Type 2 derogations are not limited only to occasional transfers. From the current derogations, this would apply to explicit consent and to the important public interest. For explicit consent, the assessment of essential equivalence is an extension of the obligation to provide information on the risks of the transfer already specified in the current wording of Article 49. The inclusion in type 2 means that consent cannot be used to circumvent the transfer rules of the GDPR, as an exporter needs to demonstrate that the transfer does not pose a risk to fundamental rights. To type 2, the amendment also adds a new derogation for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, if there are appropriate safeguards in the sense of Article 89.

Type 1 derogation: presumption of essential equivalence + limited to occasional and non-repetitive transfers	**Type 2 derogation:** data exporters must demonstrate essential equivalence
■ Contracts	■ Explicit consent
■ Legal claims	■ Important reasons of public interest
■ Vital interests of data subject	■ Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
■ Transfers from public registers	
■ Compelling legitimate interests	

The division has the advantage of aligning CJEU case law with the wording of Article 49 and Recital 111. It clarifies the burden of proof for derogations and ensures that when transferring personal data that is in itself beneficial for fundamental rights because it is in the public interest, there are means to create an appropriate balance, in particular when the transfer takes place in the context of research, archiving or statistics.[219] This aligns Chapter V with the goal of the GDPR to create a lighter regime for these "privileged purposes".[220] It should make it easier for international research and archiving projects to find a mechanism to regulate their data flows while ensuring the protection of the individuals concerned.

The change would be slight as it basically codifies CJEU case law and the text of Recital 111. The proposal would not touch upon the sequence of the transfer mechanisms — i.e., derogations of both types are only an option in case adequacy decisions and appropriate safeguards cannot be used. The exporter is responsible for demonstrating that this is the case for their envisaged transfers based on the principle of accountability.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only ~~**on one of the following conditions:**~~ **under the conditions of this Article and in full compliance with Article 44. The transferring controller or processor shall demonstrate why neither adequacy decisions nor appropriate safeguards can be used for the transfer or set of transfers in question**.

1a. An occasional and non-repetitive transfer fulfilling the conditions of paragraph 1 of this article shall only take place if one of the following conditions listed in this paragraph is met. Such a transfer is presumed to comply with Article 44. This presumption is reversible:

(a) ***(repealed)***

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's requests;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) ***(repealed)***

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. **Such a transfer shall not involve the entirety of personal data or entire categories of the personal data contained in the register. Where the register is intended for consultations by persons having a legitimate interest, the transfer shall be made only at the request of those persons of if they are to be the recipients**.

(ga) Where ~~**a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and**~~ none of the derogations **set forth in points (a) to (g) of** this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer ~~**is not repetitive,**~~ concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed **and documented** all the circumstances surrounding the data transfer, and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the

(*continued on next page*)

[217] For the research context more problems are described in a study of ALLEA. All European Academies, European Academies Science Advisory Council and Federation of European Academies of Medicine, 'International Sharing of Personal Health Data for Research' (April 2021).

[218] Articles 13(1)(f) and 14(1)(f).

[219] Kuner C., 'Data crossing borders: Data Sharing and Protection in Times of Coronavirus', Information Law and Policy Centre (27 April 2020) <https://infolawcentre.blogs.sas.ac.uk/2020/04/27/data-crossing-borders-data-sharing-and-protection-in-times-of-coronavirus-christopher-kuner/>.

[220] A need recognised at the beginning of data protection law. See Simitis S., 'Data Protection and Research: A Case Study of Control' (1981) 29(4) American Journal of Comparative Law 583 <https://doi.org/10.2307/839755>.

(*continued*)

information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

1b. Other transfers meeting the conditions of paragraph 1 shall only take place if one of the following conditions listed in this paragraph is met. The transferring controller or processor is obliged to demonstrate that the transfer or set of transfers does not undermine the level of protection of natural persons. These conditions are:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for important reasons of public interest recognized in Union or law or in the law of the Member State to which the controller is subject;

(c) the transfer is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to the implementation of appropriate technical and organisational measures.

2. (repealed)

3. Points **(b), (c) and (ga) of paragraph 1a and point (a) of paragraph 1b** shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. (repealed)

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. (repealed)

Dispute resolution by the Board (Article 65)

Lisette Mustert

Improving the effectiveness and timeliness of cross-border GDPR enforcement through meaningful involvement of the Board in investigating and settling disputes amongst DPAs

Gravity of the proposed change: moderate

Introduction

The primary responsibility for supervising compliance with the GDPR in the EU lies with the dedicated national public authorities, i.e., DPAs.[221] In case of cross-border violations of the GDPR, these authorities are required to cooperate through the GDPR's one-stop-shop mechanism.[222] In practice, it requires DPAs to reach consensus on important steps within the enforcement procedure, such as the scope of the investigation and the draft enforcement decision.[223] The EDPB — an independent EU body with legal personality[224] — plays a pivotal role in ensuring correct and consistent enforcement of the GDPR too, particularly through its dispute resolution powers.[225] This procedure is triggered, inter alia, where national DPAs are unable to reach consensus in the context of the cooperation procedure established in Article 60. Accordingly, where the lead supervisory authority does not follow objections raised by a concerned supervisory authority to its draft decision, or considers such objections not to be relevant or reasoned, the matter shall be referred to the EDPB pursuant to Article 65(1)(a). Where the EDPB settles the dispute, it does so in a binding decision addressed to the competent national DPA, which shall subsequently implement the Board's decision addressed to the data controller or processor.[226] As such, the EDPB acts as a centralised node in the GDPR's enforcement network, guiding national enforcement practices in individual cases. Hence, where the EDPB intervenes with binding decision-making powers, GDPR enforcement transcends a purely decentralised model and evolves into a system of shared enforcement where the national and EU administrations are closely integrated.[227] Consequently, the Board is an EU body with a more advanced role than many other bodies or agencies established at EU level with mere coordinating tasks.[228] However, the practical impact of an EU body's binding decision-making powers ultimately depends on its actual capacity to monitor, investigate and decide on individual cases brought before it.[229]

The amendment addresses key concerns regarding the EDPB's dispute resolution competence in light of the three phases of enforcement, i.e., to monitor, investigate and decide. These concerns relate specifically to the way the EDPB's decision making competence is triggered; the scope of its decision-making competence; its capacity to take well-informed decisions; the degree of discretion retained by national DPAs implementing the EDPB's decisions; and the mechanisms available to the EDPB to follow-up on the (correct or incorrect) implementation of its decisions at national level. Together these amendments aim to improve the effectiveness and timeliness of cross-border GDPR enforcement through involvement of the Board, mitigating the risks of administrative *inertia* in addressing cross-border GDPR violations. Where relevant, the amendments take stock of the GDPR Procedural Regulation, where little attention is paid to the EDPB's role in dispute resolution.[230]

Triggering the dispute resolution mechanism

Article 65 establishes that the dispute resolution procedure shall be triggered, inter alia, where one or more national DPAs raise a relevant and reasoned objection (RRO) to the lead authorities' draft decision, and that objection is either rejected or considered not to be relevant or reasoned.[231] Consequently, the dispute resolution procedure is only triggered at a later stage, where the draft decision has already been prepared. This timing constraints the Board's potential in contributing to effective and timely GDPR enforcement since the issues that could have been resolved earlier must wait for formal escalation at the end of the procedure. Illustrative thereof are examples from EDPB Decisions No. 3/2022, 4/2022 and 5/2022, where the Board ordered the lead authority to broaden the scope of the investigation, effectively requiring

[221] Article 55.

[222] Article 60(1).

[223] Article 60(1), Regulation 2025/2518.

[224] Article 68(1).

[225] Article 65; Docksey C., 'Article 68', in Kuner C. et al. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 1061 <https://doi.org/10.1093/oso/9780198826491.001.0001>; Hijmans H., *The EU as a constitutional guardian of internet privacy and data protection* (Springer 2016) 357 <https://doi.org/10.1007/978-3-319-34090-6>.

[226] Article 65(6).

[227] Jans JH. et al. (eds.), *Europeanisation of Public Law* (Europa Law Publishing 2015); Hofmann HCH., 'Decision-making in EU Administrative law – The Problem of Composite Procedures' (2009) 61 Administrative Law Review.

[228] As confirmed by the General Court who considered the EDPB to be more than a coordinating body only in Case T-709/21, *Whatsapp Ireland Ltd v EDPB* [2022] ECLI:EU:T:2022:783 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=ecli:ECLI:EU:T:2022:783>, para. 36.

[229] In other words, the capacity of an EU agency or body to be involved in the three stages of enforcement as identified by Vervaele in Vervaele J., 'Shared Governance and Enforcement of European Law: From Comitology to a Multi-level Agency Structure?' in Joerges C. and Vos E. (eds.), *EU Committees: Social Regulation, Law and Politics* (Hart 1999).

[230] Regulation 2025/2518 (n 4).

[231] Article 65(1)(a).

the entire process to restart.[232]

Moreover, the EDPB lacks the competence to actively monitor the progress made in individual cases and cannot step in on its own initiative, nor can it demand national DPAs to bring a case to the attention of the Board for dispute resolution. Triggering the dispute resolution procedure is up to the lead supervisory authority, who can continuously submit revised draft decisions for new rounds of consultation to the concerned authorities under Article 60(5), rather than transmitting the matter to the Board.[233] This can result in endless loops of consultation rounds, contributing to significant delays in the decision-making process.[234] The GDPR Procedural Regulation stipulates that within three months after the expiry of the deadline for DPAs to raise RROs to a draft or revised draft decision,[235] the lead supervisory authority must either submit a revised draft decision (again) or transmit the matter to the Board.[236] However, this mechanism does not resolve the underlying structural problem: it still allows for iterative "loops" of revised drafts within the deadlines, without enabling dispute resolution at earlier stages of the procedure.

To address these concerns, the amendment introduces the possibility to trigger the dispute resolution procedure either at the initiative of one or more concerned authorities or at the EDPB's own initiative provided that, based on objective reasons, a disagreement between the authorities can be established.[237] This reform allows the dispute resolution procedure to be triggered at any stage of the enforcement procedure where disputes arise in the various procedural phases of enforcement — e.g., as regards the decision to open an investigation, its scope, the required investigative actions, the decision to close an investigation, whether a violation of the law can be established, etc. This is especially important in light of the GDPR Procedural Regulation, which further operationalises continuous cooperation throughout the enforcement procedure, without effective means for escalation early in the proceeding.[238] In this way, the dispute resolution mechanism will function as a means for "peer pressure" or "mutual accountability" — a function that was advocated by the European Parliament in the trilogue negotiations of the GDPR Procedural Regulation, but rejected by the Council. Moreover, a presumed disagreement will be deemed to exist and triggers the EDPB's dispute resolution competence where a joint decision is not being taken within the procedural deadlines established by the GDPR Procedural Regulation.[239]

Important to note is that the enhanced role of the EDPB by settling disputes throughout the enforcement procedure will not encroach upon the complete independent status of DPAs. Especially as the General Court has recently confirmed that primary EU law "does not imply that the authorities of the Member States […] have absolute independence".[240] In fact, DPAs entrusted with the task to monitor compliance with the GDPR are subject to a system of mutual scrutiny between these independent authorities, which includes the EDPB; "[w]hat is important, is that the bodies scrutinizing the supervisory bodies should themselves be independent".[241]

Decisional interdependence

In practice, the EDPB's decision-making capacity is significantly constrained as it does not possess any investigative powers. Instead, the Board relies entirely upon the provision of sufficient information by the lead authority. Despite the obligation of sincere cooperation, this dependence has proven to be problematic as in all Article 65(1)(a) decisions adopted so far, the EDPB was unable to address every RRO due to an incomplete file.[242]

This stems partly from the GDPR's failure to define what constitutes a "complete file".[243] This gap will be partly remedied by the GDPR Procedural Regulation, which specifies the set of documents that the lead DPA must transmit to the Board.[244] However, difficulties remain in situations where the lead supervisory authority has not investigated issues raised by concerned authorities. Once the procedure is triggered, the Board's powers are limited: it cannot request additional information from the supervisory authorities, nor can it directly seek information from the parties under investigation.[245] As a result, in cases where the EDPB cannot settle the dispute because it lacks sufficient information, it can only order the competent authority to conduct a new investigation, causing serious delays. The GDPR Procedural Regulation introduces an important improvement by empowering the Board to request additional information from a supervisory authority.[246] However, the amendment goes further by allowing the EDPB, where necessary, to request additional information directly from the data controller, processor or data subject too. In such cases, the decision-making deadline will be extended by four weeks, to allow for the proper assessment of the additional

[232] EDPB, 'Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service' (5 December 2022) <https://www.edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202203_ie_sa_meta_facebookservice_redacted_en.pdf>; EDPB, 'Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service' (5 December 2022) <http://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf>; EDPB, 'Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited' (5 December 2022) <https://www.edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202205_ie_sa_whatsapp_en.pdf>.

[233] Articles 60(4), 63 and 65(1)(a). Cf. EDPB, 'Rules of Procedure' (Version 8, 6 April 2022), Article 11(2) <https://www.edpb.europa.eu/system/files/2022-04/edpb_rules_of_procedure_version_8_adopted_20220406_en.pdf>. If the lead DPA intends to follow the objection(s) that are deemed relevant and reasoned, it shall submit a revised draft decision to all concerned DPAs.

[234] Mustert L., *Cross-border enforcement of the GDPR by independent administrative authorities* (Doctoral thesis, University of Luxembourg 2023).

[235] In accordance with Article 60(4)(5).

[236] Regulation 2025/2518 (n 4), Art 27(1).

[237] See for a similar organization ESMA's dispute resolution procedure. Cf. Regulation 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority) [2010] OJ 2010 L 331/84, Article 19 <http://data.europa.eu/eli/reg/2010/1095/oj>.

[238] Regulation 2025/2518 (n 4), Articles 8-12.

[239] The lead DPA shall submit a draft decision to the concerned DPAs within 15 months of the lead DPA confirming its competence or of a binding EDPB decision. In cases of simple cooperation, this deadline shall be reduced to 12 months. See Regulation 2025/2518 (n 4), Article 12.

[240] Joined Cases T-70/23, T-84/23 and T-111/23, T-70/23, *Data Protection Commission v European Data Protection Board,* ECLI:EU:T:2025:116 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62023TJ0070> para. 82.

[241] Ibid.

[242] Cf. e.g., Mustert L., 'The EDPB's Second Article 65 Decision – Is the Board Stepping up its Game?' (2021) 7(3) *European Data Protection Law Review* 416 <https://doi.org/10.21552/edpl/2021/3/10>; Mustert L., 'The First Article 65 Decision – Correct and Consistent Application of the GDPR Ensured?' (2021) 7 (1) *European Data Protection Law Review* 94 <https://doi.org/10.21552/edpl/2021/1/12>.

[243] Only with regard to decision-making in accordance with Article 65(1)(a), the EDPB's Rules of Procedure Version 8 (n 233) list that the file should *at least* include the draft or revised decision; a summary of the relevant facts and grounds; the objection(s) made by the DPAs; and an indication as to whether the lead DPA does not follow the objections or considers them not to be relevant and reasoned.

[244] NOYB, 'EU to make GDPR procedures unworkable' (20 May 2025) <https://noyb.eu/en/eu-make-gdpr-procedures-unworkable>. Cf. Regulation 2025/2518 (n 4) Article 27(3).

[245] The EDPB Rules of Procedure allow this only in exceptional cases. See Article 11(2) of the EDPB Rules of Procedure (n 233).

[246] Regulation 2025/2518 (n 4), Art 27(4).

information and to enable possible hearings on the newly collected documents in accordance with Article 41 CFR, a guarantee expressly confirmed in Article 28 of the GDPR Procedural Regulation. Nevertheless, the amendment goes even further by granting an equal right to be heard to complainants, which is under the GDPR Procedural Regulation limited to instances where a complaint is rejected. This constitutes a narrower interpretation of the right to be heard than is generally applied in EU law, where the right extends to all persons adversely affected by a decision.[247] It would be erroneous to assume that complainants are only adversely affected where their complaint is rejected as situations where their claims are misunderstood, incompletely assessed or narrowly interpreted may equally have adverse effects on their rights and interests.

In exercising these powers, the EDPB must naturally fully respect the fundamental rights of the parties involved, including the presumption of innocence, particularly where the proceeding may be considered to involve a criminal charge. Only with such a transfer of powers, consistency and convergence in the enforcement of EU data protection laws can be effectively established.[248]

Shared enforcement: discretion everywhere

Finally, concerns can be raised as to whether and to what extent a national supervisory authority complies with the EDPB's binding decisions, particularly due to the broad discretion left to the national supervisory authority in their implementation, and the EDPB's limited capacity to act when implementation is delayed, incomplete or incorrect. First, although some EDPB decisions exert strong influence upon the national authorities — such as requiring to include a specific infringement in a national decision[249] — other aspects may leave broad discretion to the national supervisory authorities — especially the calculation of the proposed administrative fine, and in general the proposed enforcement action. As a result, despite the binding nature of the Board's decisions, their impact may be restraint, which led the General Court to characterise EDPB decisions to be merely preparatory in nature[250] — a judgment currently pending in appeal before the CJEU.[251]

Second, the EDPB is not required to actively monitor whether the supervisory authorities live up to the Board's directions in its binding decisions. Under the current framework, national DPAs are only required to inform the Board of the date of notification of the final decision to the parties involved.[252] To address this gap, the amendment allows the EDPB to direct its decision towards a data controller or processor — instead of the competent DPA — insofar as the national supervisory authorities have not complied with the Board's decision.[253] In other words, to exercise direct enforcement powers against a market participant, without interference of the competent supervisory authority. This reform would significantly limit the national authorities' discretion and shift their role akin to that of a subcontractor of the EDPB.[254] This also means that, in case of non-compliance by the national supervisory authorities, the EDPB will be the first body to intervene in national decision-making and take over such task without having only the Commission or the CJEU to ensure the national supervisory authorities compliance with the Board's decision.

It should be noted that the amendment significantly expands the competences of the Board, strengthening its capacity to intervene more effectively and at earlier stages of cross-border enforcement procedures. This extension of powers inevitably translates into a corresponding increase in workload, requiring the Board to devote additional resources to the assessment and collection of information, the organization of hearings, and the resolution of disputes. Given that the EDPB's budgetary situation was already under strain in 2023,[255] the enhanced responsibilities introduced by these amendments make a corresponding increase in financial and human resources indispensable in order to ensure the effective exercise of its mandate and to safeguard the uniform application of the GDPR across the EU.

Article 65

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where **the lead or any concerned authority disagrees about the procedure or content of an action or inaction of a competent authority of another Member State~~, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation~~;**

(aa) where the Board establishes, on the basis of objective criteria, a disagreement between the lead and concerned authorities. Disagreement is presumed where a joint decision is not being taken within the procedural deadlines established by the Regulation (EU) No. 2025/2518;*

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

1a. At the request of the Board, the competent authority shall provide the Board with all necessary information to carry out its dispute resolution competence, provided that it has legal access to the information, and that the request is necessary in relation to the dispute resolution competence.

1b. Where information is not available or is not made available by the competent authority in a timely fashion, the Board may address a duly justified and reasoned request to other supervisory authorities of the Member States concerned.

1c. Where information is not available or is not made available under paragraph 1a or 1b in a timely fashion, the Board may address a duly justified and reasoned request directly to the relevant data controller, data processor, or data subject. The reasoned request shall explain why the information is necessary.

1d. Prior to adopting the binding decision pursuant to paragraph 1, the Board shall provide the data controller, processor and data subject with the opportunity to make their views known in writing on any new factual or legal elements. The Board shall set an appropriate time limit not shorter than two weeks. The period for the adoption of the binding decision pursuant to paragraph 1 shall be suspended until the parties under investigation and the data subject have made their views known or until the expiry of the time limit referred to in this paragraph.

(*continued on next page*)

[247] Case T-183/23, *Ballmann v European Data Protection Board*, ECLI:EU:T:2025; 735 <https://curia.europa.eu/juris/document/document.jsf?text=&docid=302501&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=879455> para. 61.

[248] Spendzharova AB., 'Becoming a powerful regulator: the European Securities and Markets Authority (ESMA) in European Financial Sector Governance' (2017) 8/2017 TARN Working Paper 11,

[249] Cf. e.g., EDPB, 'Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR' (28 July 2021), paras. 66, 199 and 201 <https://www.edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf>.

[250] Case T-709/21, *Whatsapp Ireland Ltd v EDPB* (n 228) para. 42.

[251] See pending Case C-97/23 P *Whatsapp Ireland Ltd v EDPB.*

[252] Article 65(6).

[253] See for a discussion of a similar transfer of power in the area of banking supervision Timmermans J., and Chamon M., 'Controlling the SRB's resolution powers', in Scholten M., and Brenninkmeijer A. (eds.), *Controlling EU Agencies: The Rule of Law in a Multi-jurisdictional Legal Order* (Edward Elgar 2020) 293 and 311 <https://doi.org/10.4337/9781789905427>.

[254] Jans et al. (n 227) 94-102.

[255] EDPB and EDPS, 'Open letter on EDPB budget proposal for 2023' (12 September 2022) < https://www.edpb.europa.eu/system/files/2022-09/letteronbudget_out2022-0068.pdf>.

(*continued*)

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter **or where additional information was requested**. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.
3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.
4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.
5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.
6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of **the decision taken and** the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.
7. **Without prejudice to the powers of the Commission under Article 258 of the Treaty on the Functioning of the European Union (TFEU), where a competent authority does not comply with the decision of the Board, and thereby fails to ensure that a data controller or processor complies with the requirements directly applicable to it, the Board may adopt an individual decision addressed to a data controller or processor requiring the necessary action to comply with its obligations under Union law, including the cessation of any practice.**

—

* OJ L 2015/2518, 12.12.2025.

Representation of data subjects (Article 80)

Gianclaudio Malgieri
Reinventing data subject representation for participatory data governance
Gravity of proposed change: serious

Good

Article 80 represents an important recognition of the structural asymmetries between individuals and powerful data controllers. It allows data subjects to mandate not-for-profit organisations to act on their behalf in exercising rights and seeking remedies. This principle has been rightly praised as a pioneering step toward collective enforcement, particularly in Member States such as the Netherlands, France or Germany, where legal cultures are more open to representative action. These provisions are crucial in ensuring access to justice in data protection and in supporting individuals who are structurally disadvantaged.[256]

Challenge

Yet, Article 80 remains under-implemented, under-used and conceptually narrow. In its current form, it is limited to *ex post* representation in complaints or legal remedies and fails to realise the transformative potential of collective data subject agency. The GDPR, both in its initial provisions and in its remedies, omits the possibility for representatives to proactively negotiate the terms and conditions of data processing, to engage with controllers on the choice of lawful bases, and to collectively exercise rights of access, erasure, rectification, objection, restriction, portability, or protection from automated decision-making.

More broadly, this provision fails to reflect the core insight that data protection is not only about information and consent, but about power imbalance. Consent, long considered a cornerstone of data protection, has become a fallacious safeguard in many digital contexts.[257] It is plagued by consent fatigue, dark patterns and the privacy paradox, where individuals express concern for their privacy but feel compelled to accept invasive practices due to a lack of alternatives.[258] Meanwhile, top-down lawful bases such as contract or legitimate interest are often dictated unilaterally by the controller, with little transparency or opportunity for negotiation.

By contrast, the Data Governance Act (DGA) introduces the concept of data cooperatives (Article 2(15)), defined as organisational structures constituted by data subjects or small and medium enterprises (SME) that support their members in exercising data rights, negotiating processing conditions, and making informed choices before consent.[259] The DGA thus provides an institutional blueprint for participatory data governance, which the GDPR still lacks. However, in the DGA, there is nothing more than a definition for data cooperatives, with no related rights, duties or operational rules.

It is worth recalling that the Representative Actions Directive (EU) 2020/1828 requires every Member State to provide "qualified entities" with a procedural route to bring representative actions, both injunctive and redress measures, against "traders" for infringements of a long list of EU laws; crucially, Annex I expressly includes the GDPR.[260] In other words, where GDPR non-compliance harms consumers, designated organisations can already sue to stop the practice and obtain compensation or other redress on a collective basis. However, the Directive is structurally limited to consumer–trader contexts and is largely *ex post* and litigation-centred: it does not create mechanisms for collective, *ex ante* participation in decisions about purposes, lawful bases or safeguards, nor does it enable collective exercise of the substantive data-subject rights under Articles 15–22.

Solution

Article 80 should therefore be reformed to:

[256] Malgieri (n 173).

[257] Schermer BW. et al., 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16 Ethics and Information Technology 171 <https://doi.org/10.1007/s10676-014-9343-8>; Barocas S., and Nissenbaum H., 'On Notice: The Trouble with Notice and Consent' [2009] Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information 7; van der Hof (n 56).

[258] Ducato R., and Marique E., 'Come to the Dark Side: We Have Patterns. Choice Architecture and Design for (Un)Informed Consent' (2019) SSRN <https://papers.ssrn.com/abstract=3365952>.

[259] Mannan Me et al., 'Data Cooperatives in Europe: A Preliminary Investigation' (2022) 24 Network Industries Quarterly <https://www.network-industries.org/wp-content/uploads/2022/10/Data-Cooperatives-in-Europe.pdf>.

[260] Directive 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L409/1 <http://data.europa.eu/eli/dir/2020/1828/oj>.

a) Expand the mandate of Data Subject Representatives (DSRs) to include collective exercise of all substantive data subject rights under Articles 15–22, in addition to procedural rights to lodge a complaint and ask for compensation;
b) Empower DSRs to participate in negotiations over lawful bases under Article 6, especially consent and legitimate interest;
c) Require that controllers consult DSRs during a DPIA, in line with Article 35(9), where high-risk processing affects identifiable groups;
d) Mandate that Member States establish structural funding mechanisms to support the functioning of DSRs, including data cooperatives, recognising their role in protecting the public interest and balancing structural inequalities in data governance.

This model would empower representative entities not only to protect individuals but to recalibrate power asymmetries through institutionalised, pre-emptive participation.

Justification

The GDPR is premised on fundamental rights, yet its architecture is often seen as individualistic and reactive. In practice, the enforcement of data protection rights is too often dependent on either under-resourced public authorities or isolated individuals. Neither approach is adequate in contexts of massive asymmetries in information, resources and bargaining power.

A revised Article 80 would recognise that collective empowerment is not a procedural luxury, but a substantive necessity.[261] Just as collective bargaining in labour law corrects workplace inequalities, so too can collective data subject representation correct systemic dependencies in the digital economy.[262] This is especially needed in platform environments, where users often lack genuine alternatives and face complex, high-stakes processing scenarios involving profiling, scoring and behavioural inference.[263]

Moreover, public financing of DSRs is essential. These entities provide public value by acting as intermediaries of accountability and fundamental rights. Much like courts, ombudsmen or consumer protection authorities, they contribute to the democratic governance of digital infrastructures. Structural funding, possibly linked to the regulator's budget or to a dedicated legal aid-like scheme, would ensure independence, continuity and equitable access to collective representation.

Operationally, the mandate for DSRs to "participate in negotiations over lawful bases" would piggy-back on existing GDPR touchpoints and the proposed Article 80 revision. To make this workable, a controller that plans large-scale or high-risk processing affecting a clear group must invite any relevant data subject representatives to a short consultation alongside a DPIA. The outcome might be a simple public term sheet that fixes the purpose, the chosen lawful basis and its limits, the safeguards and the default user controls. For consent, representatives help design the user journey so that consent is unbundled and granular and there is an equivalent path that uses less personal data, so refusal brings no disadvantage. For legitimate interests, representatives help draft the assessment, narrow the purpose, test less intrusive options, set opt-out as the default for uses that are not essential and agree on measurable safeguards such as retention limits and exclusion of sensitive features. The term sheet is attached to the record of processing and to the data protection notice, giving regulators a clear yardstick. This replaces countless weak take-it-or-leave-it prompts with one negotiated baseline that changes defaults and gives data subjects real power before processing begins.

Article 80
Representation of data subjects **and participatory governance**
1. The data subject shall have the right to mandate a not-for-profit body, organisation, or association, **including a data cooperative as defined under Regulation (EU) 2022/868**,* which has been properly constituted in accordance with the law of a Member State, has statutory objectives in the public interest, and is active in the field of data subject rights and freedoms ~~**with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.**~~ to:
(a) exercise on their behalf any of the rights referred to in Articles 15 to 22;
(b) lodge a complaint and exercise the rights referred to in Articles 77, 78, 79 and 82;
(c) engage in prior negotiation with controllers concerning the purposes and conditions of processing, including the lawful bases under Article 6(1), in particular consent and legitimate interest.
2. Member States ~~**may**~~ **shall** provide that any body, organisation or association referred to in paragraph 1, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.
3. The body, organisation or association referred to in paragraph 1 may also be consulted by the controller, together with the data subjects concerned, during the assessment and consultation phases of the data protection impact assessment referred to in Article 35(9), where processing operations are likely to result in a high risk to the rights and freedoms of natural persons.
4. Member States shall establish appropriate funding mechanisms to support the functioning and independence of the bodies referred to in paragraph 1, recognising their contribution to the collective exercise of fundamental rights and the public value they provide in the democratic governance of personal data.
—
* OJ L 152, 3.6.2022, p. 1.

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 89)

Heidi Beate Bentzen

Improving the legal conditions for scientific research in the EU whilst increasing the protection of research participants

Gravity of the proposed change: moderate

Introduction

A main challenge with research and technological development is that the EU shares competence to regulate these areas with the Member States.[264] This has led to diverging regulation and interpretations across the EU, an issue which has become particularly evident through the process of setting up secondary use of health data through the European Health Data Space (EHDS).[265] The most significant improvement in the conditions for conducting scientific research in the EU would only be possible if the EU had wider competence to harmonise this legal field across Member States. Nevertheless, one of the objectives of the EU is to

[261] Kaminski ME., and Malgieri G., 'Impacted Stakeholder Participation in AI and Data Governance' (2024) SSRN <https://papers.ssrn.com/abstract=4836460>.
[262] Directorate-General for Employment, Social Affairs and Inclusion (European Commission) et al., *Study Exploring the Context, Challenges, Opportunities, and Trends in Algorithmic Management in the Workplace: Final Report* (Publications Office of the European Union 2025) <https://data.europa.eu/doi/10.2767/5629841>.
[263] Aloisi A., 'Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights' (2024) 40 International Journal of Comparative Labour Law and Industrial Relations <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\IJCL\IJCL2024001.pdf>.
[264] Article 4(3) TFEU.
[265] TEHDAS Towards European Health Data Space, 'Deliverable 5.2 Recommendations for European countries when planning national legislation on secondary use of health data' (1 March 2023) <https://tehdas.eu/results/tehdas-study-member-states-to-harmonise-national-legislation-to-enable-the-secondary-use-of-health-data/>.

strengthen its scientific and technological bases by the free circulation of "researchers, scientific knowledge and technology" and to "become more competitive, including in its industry".[266] To achieve this purpose, the EU shall support free cooperation and industry exploitation across borders, inter alia through removal of legal obstacles to that cooperation.[267] The EU also aims to ensure protection of fundamental rights, which can be challenged by some scientific research activities. Hence, the GDPR has a twofold objective to: (1) protect fundamental rights and freedoms — and, in particular the right to personal data protection — while at the same time (2) neither restricting nor prohibiting the free movement of personal data within the EU.[268] This twofold objective of the GDPR has been further specified in its provisions to facilitate scientific research through a range of derogations.[269]

Definition of scientific research

Hence, scientific research enjoys a privileged position in the GDPR. It is stated in its preamble that scientific research purposes should be interpreted broadly and should also cover, for instance, privately funded research.[270] However, the very vague guidance provided in the preamble — and the fact that this is only touched upon in the preamble and not in the enacting provisions — does not create the necessary definitional boundaries to justify the GDPR derogations to data subject rights (cf. Article 89(2)).

Therefore, the amendment includes a clear definition of "scientific research" in Article 4. This definition is important both to protect data subjects' fundamental rights and to protect society from actors misusing a guise of scientific research to take advantage of lenient derogations. This will in turn contribute to maintain legal certainty and trust in genuine scientific research. The definition is a very slightly edited version of the definition of "scientific research" in the UN Special Rapporteur on the Right to Privacy's Recommendation on the Protection and Use of Health-Related Data (2019).[271] That Recommendation's definition, in turn, built on the Organisation for Economic Co-operation and Development (OECD) Frascati Manual (2015),[272] combined with a review of CJEU and European Court of Human Rights (ECtHR) jurisprudence on the subject matter which the author conducted in an effort to distil potential assessment criteria for what constitutes scientific research.[273]

The criteria for determining whether an activity is scientific research were adopted in full by the UN Special Rapporteur on the Right to Privacy and the amendment introduces the same factors into the GDPR. Three factors were derived from jurisprudence: (1) the role of the legal entity where the activity is carried out; (2) the role of the natural person (s) carrying out the activity; and (3) quality standards, including use of scientific methodology and scientific publication.[274] In addition, the amendment adds a fourth factor (which was also included in the Recommendation): adherence to research ethical norms.[275]

Pseudonymisation

Anonymous or anonymised data is defined antithetically in Article 4 (1) and interpretative guidance is provided in Recital 26, inter alia stating that the "principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". Researchers are rarely interested in the identity of the research subjects. But anonymous or anonymised data usually lack the necessary utility, richness and linkage possibilities needed for scientific progress, and datasets often include uniquely identifiable personal data such as genomic data which cannot be anonymised. Hence, for scientific research purposes, data are most often processed pseudonymously. According to Article 89, processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be subject to appropriate safeguards. Pseudonymisation is included as an example.

A typical scientific dataset today contains many data points and would provide the possibility for reidentification of research participants on the basis of the variables alone, through linkage with publicly available datasets, or through the inclusion of uniquely identifiable data. The reidentification literature is brimming with examples showing the ease with which adversaries can reidentify research participants and the most recent literature also makes use of AI to assist with the reidentification.[276] Researchers — and even more so funders and publishers — tend to forget that the EU open science policy not only aims to ensure that the data are as open as possible, but also as closed as necessary.[277] Rich datasets of pseudonymised data are frequently made openly available with the risks that entail to research participants on the faulty assumption that it is impossible or only theoretically possible to reidentify research participants.

Pseudonymisation was one of the areas where the Member States had diverging interpretations under the DPD. Therefore, particularly from the UK, one might find old papers referring to pseudonymous data as anonymous. With the advent of the GDPR, a definition of pseudonymisation was included in Article 4(5), which appeared to settle the matter that pseudonymized data are personal data. CJEU jurisprudence such as *Breyer*[278] and *Nowak*[279] seemed to confirm this. However, with *SRB*, unacceptable uncertainty and confusion arose again.[280] The *SRB* judgment was appealed, with the appeal judgment being more in line with

[266] Article 179(1) TFEU.
[267] Article 179(2) TFEU.
[268] Article 1.
[269] Bentzen HB., and Høstmælingen N., 'Balancing protection and free movement of personal data: the new European Union General Data Protection Regulation' (2019) 170 Annals of Internal Medicine 335–337 <https://doi.org/10.7326/M18-2782>.
[270] Recital 159.
[271] United Nations Special Rapporteur on the Right to Privacy, 'Recommendation on the Protection and Use of Health-Related Data' (2019) <https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf>.
[272] Organisation for Economic Co-operation and Development, 'Frascati Manual 2015' (2015) <https://www.oecd.org/en/publications/2015/10/frascati-manual-2015_g1g57dcb.html>.
[273] Bentzen HB., 'In the Name of Scientific Advancement: How to Assess what Constitutes 'Scientific Research' in the GDPR to Protect Data Subjects and Democracy' in Terzis G. et al. (eds.), *Disinformation and Digital Media as a Challenge for Democracy* (Intersentia 2020) 341-366 <https://doi.org/10.1017/9781839700422>.
[274] Ibid.
[275] Ibid.
[276] E.g., Na L. et al., 'Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning' (2018) 1(8) *JAMA Netw Open* <https://doi.org/10.1001/jamanetworkopen.2018.6040>.
[277] E.g., European Commission, 'Open science' <https://rea.ec.europa.eu/open-science_en>.
[278] Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* ECLI:EU:C:2016:779 [2016] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0582>.
[279] Case C-434/16 *Peter Nowak v. Data Protection Commissioner* ECLI:EU:C:2017:994 [2017] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2017%3A994>.
[280] Case T-557/20 *Single Resolution Board v. European Data Protection Supervisor* ECLI:EU:T:2023:219 [2023] <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62020TJ0557>.

CJEU jurisprudence.[281] Nevertheless, the interpretation is complex and it requires in-depth understanding of the dataset, linkage possibilities, and the reidentification literature – which most lawyers lack – to avoid a situation in scientific research where extremely large datasets with special categories of personal data are processed in a manner that places data subjects at risk of being identified. Hence, the amendment adds a new Article 4(5a) to specify that pseudonymised data remain personal data, also in cases where the data may appear anonymous on someone's hand. This would prevent datasets where individuals are identifiable to be made openly available. The EDPB has phrased this well in their recent guidelines on pseudonymisation.[282] Hence, the amendment uses a slightly edited version of their phrasing as the new definition.

Furthermore, Recital 162 should be corrected to clarify that aggregated and anonymous data are not synonyms: the "statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate*d anonymous* data…". Aggregation is a statistical method that can be used for presenting data in an anonymised manner, however, the method does not always render the data anonymous.[283] Data can be aggregated without being anonymous, particularly if there are very few data subjects in a dataset.[284] This is a problem often encountered in rare disease research, or when having to present international data on rare disease cases and there is only one such rare disease case in a country.

Other appropriate safeguards

Apart from pseudonymisation, examples of other appropriate safeguards are not mentioned in the current text of the GDPR. PETs could, for instance, have been specifically mentioned here. However, the main omission is that informed consent to research participation as a research ethics tool is not mentioned as a safeguard despite being core to human dignity and the right to the integrity of the person as enshrined in the CFR.[285] Including this safeguard could also help clarify that informed consent to research participation is a research ethics tool and not an instrument for data protection compliance.[286] A lawful basis for data processing can, but does not need to be, consent. In cases where the lawful basis for data processing is consent, this can be combined with the informed consent to research participation, however, they remain separate instruments with separate historical backgrounds and legal bases. The amendment hence suggests a relevant addition to Article 89. Furthermore, it should be added to Recital 156 that "[i]nformed consent to research participation is a research ethics instrument. It is not an instrument for data protection compliance but an additional safeguard where personal data are processed for scientific research purposes". One might consider instead clarifying this in guidance, however, given the high number of non-lawyers consulting the GDPR on this particular issue, combined with the high degree of misunderstanding related to the issue, adding this clarification to Article 89 and to the relevant recital would be beneficial not just for researchers but also for the protection of research participants.[287]

Benefit sharing

To increase societal acceptability for wide use of personal data for scientific research purposes by the private sector, benefit sharing measures should be in place, and the amendment therefore adds them to Article 89. Research shows that Europeans are reluctant to have their personal data processed by private entities, but that they find the processing more acceptable if not only the purpose is considered good but that there also are benefit sharing measures in place for the individuals concerned or for society.[288] People do not want all benefits to go to a private company's shareholders.[289] An example of a benefit sharing measure is when a pharmaceutical company uses health registry data of the inhabitants of a country to conduct research related to a new drug and the company gives a discount when the drug is sold to the health care system in that country.

Article 4
Definitions
[…]
(5a) 'pseudonymised data' means personal data which could be attributed to a specific data subject with the use of additional information, having regard to the means reasonably likely to be used by the controller or by another person. This also applies if pseudonymised data and additional information are not in the hands of the same person. Even if all additional information retained by the pseudonymising controller has been erased, the pseudonymised data become anonymous only if the conditions for anonymity are met;
[…]
(29) 'scientific research' means an activity that satisfies all of the following:
(a) creative and systematic work undertaken to increase the stock of knowledge and/or to devise new application of available knowledge;
(b) novel, creative, uncertain, systematic, and transferable and/or reproducible activity;
(c) factors for determining whether an activity is scientific research include the role of the legal entity where the activity is carried out; the role of the natural person(s) carrying out the activity; quality standards including use of scientific methodology and scientific publication; and adherence to research ethical norms;
(d) research within any discipline that may process personal data, including medical and health sciences, natural sciences, engineering and technology, social sciences, humanities and fine arts, is scientific research;
(e) the scientific research may be basic research, applied research or experimental development, and policy analysis and epidemiology are both examples of scientific research;
(f) scientific research can be both publicly and privately funded and conducted, and may in some cases be conducted for profit;

(*continued on next page*)

[281] Case C-413/23 P *European Data Protection Supervisor v. Single Resolution Board* ECLI:EU:C:2025:645 [2025] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0413>.

[282] EDPB, 'Guidelines 01/2025 on Pseudonymisation' (16 January 2025) para. 22 <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en>.

[283] Agencia Espanola Protección Datos & European Data Protection Supervisor, '10 Misunderstandings related to Anonymisation' (2021) <https://www.edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en> and Xu F. et al., 'Trajectory Recovery from Ash: User Privacy Is NOT Preserved In Aggregated Mobility Data' (2017), Proceedings of the 26th International Conference on the World Wide Web (WWW '17), International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 1241-1250 <https://doi.org/10.1145/3038912.3052620>.

[284] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (11 April 2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

[285] Articles 1 and 3 Charter (n 26).

[286] EDPB, 'Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))' (23 January 2019) <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en>.

[287] Dove E.S. and Chen J., 'Should consent for data processing be privileged in health research? A comparative legal analysis' (2020) *International Data Privacy Law* <https://doi.org/10.1093/idpl/ipz023>.

[288] Shah N. et al., 'Governing health data across changing contexts: A focus group study of citizen's views in England, Iceland, and Sweden' (2021) International Journal of Medical Informatics <https://doi.org/10.1016/j.ijmedinf.2021.104623>; Johansson JV. et al., Publics' preferences for sharing health data: a discrete choice experiment' (2021) JMIR Medical Informatics <https://medinform.jmir.org/2021/7/e29614>; Biasiotto R. et al., 'Public preferences for digital health data sharing: a discrete choice experiment in 12 European countries' (2023) Journal of Medical Internet Research <https://doi.org/10.2196/47066>.

[289] Ibid.

(*continued*)

Article 89
Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
[…]
1a. Processing for scientific research purposes shall be subject to appropriate safeguards to protect human dignity and the right to integrity of natural persons. Those safeguards may include measures such as ethics approval and informed consent to research participation. Processing for scientific research purposes by private companies should be subject to benefit sharing measures.
[…]

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

LD: The open access publication of this research was supported by the Starting Grant for LD of KU Leuven (ZKE5533). Sincere gratitude to Emma Aldibs for her proofreading support.

DK is a postdoctoral researcher of the *Fonds de la Recherche Scientifique – FNRS*. Many thanks to Guglielmo Finotti, Juraj Sajfert and Heidi Waem for their useful comments.

EF: This research was supported by the *Fonds voor Wetenschappelijk Onderzoek – Vlaanderen* (FWO) under the Grant Agreement No. G039725N. I extend my sincere gratitude to Prof. Simone van der Hof, Tatiana Duarte Nicolau, and Charlotte Somers for their invaluable feedback on previous versions of my contribution, as well as to Emma Aldibs for the proofreading.

JR: This research was supported by the Working Group on Internet Governance and Regulation of the Research Network on Internet, AI and Society (GDR 2091) of the *Centre national de la recherche scientifique* (CNRS).

HBB is funded by the EU EIC grant No. 101071203 and the Research Council of Norway projects Nos. 322672 and 353207.

Data availability

No data was used for the research described in the article.