

The Abuse & Misuse of the GDPR Right of Access: Refining the Sharp Edges of the Digital Omnibus Proposal

Larisa-Mădălina Munteanu*

Keywords: GDPR; right of access; abuse and misuse of right; Digital Omnibus; harmonisation.

One of the most controversial points originating from the EU Digital Omnibus proposal was regulating the abuse of the right of access, as framed by Article 12(5) GDPR, read together with Article 15 GDPR. In light of the incompatibilities which came to light, this article will employ doctrinal and comparative legal analysis for promoting harmonisation with minimal regulatory costs. This approach establishes a dual framework distinguishing between abuse and misuse of the right of access, strengthening the framework under which data controller could counter malicious access requests.

By relying on the abuse of rights doctrine and practical examples, it is proposed that the two concepts are defined by legitimacy: abusing this right would mean exercising it outside the sphere of the law (e.g. concealing malware attacks), whereas misusing it would rely on a legitimate purpose other than data protection (e.g. research, evidence-gathering). This criterion will also revitalise the objective-subjective test for assessing abuse of access rights, making the requester's intention relevant only insofar as it falls within or outside the bounds of legitimacy and avoiding a 'shield' for blanket refusals.

* Director and Data Protection Lawyer at Protector PriVit S.R.L.; PhD Researcher at Erasmus Graduate School of Law, Erasmus University Rotterdam, the Netherlands. For correspondence: <munteanu@law.eur.nl>.

I. Introduction

The ten-year milestone from establishing the ‘gold standard’ of worldwide data protection¹ is soon to be reached. The EU General Data Protection Regulation (‘GDPR’)² was adopted in 2016, enforceable since 2018, and reviewed in 2025 through the Digital Omnibus (‘the proposal’) as part of simplification efforts of the European Commission (‘EC’).³ In essence, the EC attempted to counter the developing pattern of data protection requests which are motivated by bad faith, observed already in the early post-GDPR years.⁴

Since the GDPR’s proposed changes specifically target the reinterpretation of Article 12(5) GDPR in cases of abusive data subject access requests, it is worth considering how to address potential regulatory (mis)alignment. Therefore, the scope of this article is deliberately limited to applications of Article 15 GDPR, which regulates the right of access, examined in conjunction with Article 12(5) GDPR, which allows data controllers to charge a reasonable fee or to refuse to comply with ‘manifestly unfounded or excessive requests’.⁵

As a matter of terminology, ‘ius accessus’ will be used interchangeably with the ‘right of access’, and ‘abusus’ with its abuse. Exercising this right will be subsequently referenced as ‘access requests’ or ‘requests of access’ alternatively. Nonetheless, as the abuse of right theory will support the analytical framework, only cases in which the requester is the holder of the right of access will be subject to analysis, be it as a data subject or as a third party acting on their behalf with an authorisation, such as parents acting on behalf of their children or solicitors acting on behalf of clients.⁶ In the end, there can be no abuse of a right where no right exists.⁷

¹ Chris Moschovitis, ‘European Regulations’ in Chris Moschovitis (ed), *Privacy, Regulations, and Cybersecurity* (John Wiley & Sons 2021) 89-117, 106 <<https://doi.org/10.1002/9781119660156.ch6>>.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

³ European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024’ COM(2025) 837 final, 19 November 2025 (Digital Omnibus).

⁴ Emily Jones, ‘The GDPR Two Years On’ (2020) 35(1) *Antitrust* 51-57, 55 <<https://www.jstor.org/stable/27182525>> accessed 21 June 2026.

⁵ Data controllers can limit data subject access requests under Articles 12(5) or 23 GDPR, both of which also apply to other Chapter III rights. Article 57(4) GDPR provides a corresponding limitation for requests to data protection supervisory authorities. However, the Digital Omnibus proposal, together with doctrine and case law, primarily associates abuse of access rights with Article 12(5) GDPR, as supervisory authorities’ operations present an isolated case. Accordingly, this article builds on that acquis without disregarding the potential relevance of Articles 23 or 57(4) GDPR to abusive requests.

⁶ European Data Protection Board, ‘Guidelines 01/2022 on data subject rights - Right of access’ (Version 2.1, 28 March 2023) <https://www.edpb.europa.eu/system/files/documents/2023-04/edpb_guidelines_202201> accessed 8 February 2026.

⁷ For the opposing view, it has been suggested that abusing the right of access is incidental even in cases of impersonation attacks, although the attacker inherently acts without an authorisation; see Cédric Lauradoux, ‘Can Authoritative Governments Abuse the Right to Access?’ in Agnieszka Gryszczyńska and others (eds), *Privacy Technologies and Policy* (Springer 2022) 23-33 <https://doi.org/10.1007/978-3-031-07315-1_2> accessed 19 September 2026.

Methodologically, doctrinal and comparative legal analysis will be used, showcasing an exploratory and progressive view over the Digital Omnibus with respect to abusive data subject access requests. This contribution will address and reconcile the tensions between the different positions adopted by EU bodies on what constitutes an abusive request. Although the abusive exercise of rights is a chameleon that changes colours across jurisdictions, this article will not elaborate on these perspectives. Instead, it uses this theory as an analytical tool to promote regulatory coherence and limit the fragmentation the EU proposal may cause.

In essence, building on criticism originating from both private and public sector, this article will advance an interpretation for harmonising the solutions offered by, on one hand, the Court of Justice of the EU ('CJEU'), and, on the other hand, the European Data Protection Board ('EDPB') with the EC. Drawing on similar attempts in intellectual property, this article will propose a dichotomy between abuse and misuse of access rights, grounded in practice and regulatory frameworks rather than speculation. This distinction will guide data controllers in responding to access requests, by using a criterion of legitimacy to separate requests they may reject or charge for (abuse) from those they should comply with (misuse). The system operates on the presumption that requests should be complied with, even where the exercise of the right is not connected to data protection, unless the controller can establish illegitimate intention, thereby rendering it abusive.

Ultimately, irrespective of the outcome of the proposal, the findings of this article are likely to be of significant interest to organisations worldwide, in particular due to the so-called 'Brussels effect',⁸ which could extend to regulating the abusive exercise of access rights. An example of how this effect influenced the responses to data protection rights in non-EU business was highlighted in a study focused on Canada, which concluded that post-GDPR access requests had a higher response rate.⁹

II. Unveiling the Abusive Data Subject Access Requests in light of the Digital Omnibus

1. *Ius Accessus et Abusus*: Ante Digital Omnibus

Originally, the rights derived from the GDPR, and more broadly, even the GDPR itself, are the fruit of the seed planted earlier through Article 8 of the Charter of Fundamental Rights of the European Union¹⁰, although earlier legal instruments set the foundation.¹¹ The right of access is incorporated in

⁸ Anu Bradford, 'The Brussels Effect' (2012) 107 *Northwestern University Law Review* 1-68 <<https://scholarship.law.columbia.edu/books/232>> accessed 22 June 2026.

⁹ René Mahieu and others, 'Measuring the Brussels Effect through Access Requests: Has the European General Data Protection Regulation Influenced the Data Protection Rights of Canadian Citizens?' (2021) 11 *Journal of Information Policy* 301-349 <<https://doi.org/10.5325/jinfopoli.11.2021.0301>> accessed 22 June 2026.

¹⁰ Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

¹¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 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, art 12; OECD, 'Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (23 September 1980) C(80)58/FINAL, 37.

the second paragraph of this legal provision.¹² Accordingly, the right of access was considered the facilitator and cornerstone of the other rights provided by data protection regulations,¹³ likewise recognised by the CJEU in the *F.F. v Österreichische Datenschutzbehörde and CRIF GmbH* case.¹⁴

Additionally, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data includes provisions about the data subjects' right to access the data.¹⁵ Outside the EU, as discussed in a 2019 hearing before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, this right has even been considered a bridge for various regulations since 'the GDPR, the California Consumer Privacy Act, the Fair Credit Reporting Act, and other privacy laws around the world do share one thing in common: giving people a right to access their data'.¹⁶

Even so, it should not be disregarded that 'law is brought into being for the benefit of the community and not for the advantage of the individual'.¹⁷ As a result, malicious or unlawful intention, according to the French school of thought, pioneer of the abuse of right doctrine in European continental law,¹⁸ deserves no legal protection.¹⁹ Although the abuse of right theory 'finds application in practice to a somewhat uncertain degree',²⁰ the current article will transpose it into the real-life environment using case law and doctrinal examples (i.e. the different intention - different result matrix detailed in section III), reframing it in the context of data subject access requests.

The relationship between the actors involved will be limited to a natural person (data subject) and a legal person or another natural person (data controller), as defined under Article 4 GDPR. Abuse is frequently observed on the side of the legal persons acting as data controllers, both private and public, such as in cases of abuse of dominant power,²¹ abusive data collection practices,²² abusive identity

¹² 'Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'.

¹³ Bart Custers and Anne-Sophie Heijne, 'The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in Theory and Practice' (2022) 46 *Computer Law & Security Review* 105727 <<https://doi.org/10.1016/j.clsr.2022.105727>>.

¹⁴ Case C-487/21 *F.F. v Österreichische Datenschutzbehörde and CRIF GmbH* [2023] ECLI:EU:C:2023:369.

¹⁵ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 28 January 1981, entered into force 1 October 1985) ETS 108.

¹⁶ United States Senate Committee on Banking, Housing, and Urban Affairs, 'Privacy rights and data collection in a digital economy' (Hearing before the United States Senate, 116th Congress, 1st session, 7 May 2019, Washington, DC: U.S. Government Publishing Office) <<https://www.govinfo.gov/content/pkg/CHRG-116shrg39483/html/CHRG-116shrg39483.htm>> accessed 2 February 2026.

¹⁷ H C Gutteridge, 'Abuse of Rights' (1933) 5 *Cambridge Law Journal* 22-45, 27 <<https://doi.org/10.1017/S0008197300128521>>.

¹⁸ Filippo Ranieri, 'Abuse of Law' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2012) <https://max-eup2012.mpipriv.de/index.php/Abuse_of_Law> accessed 17 June 2026.

¹⁹ Louis Jossierand, *De l'esprit des droits et de leur relativité: Théorie dite de l'abus des droits* (Dalloz 1939).

²⁰ Gutteridge (n 17) 32.

²¹ Alexandre Köhler, 'Online Advertising and the Competition for Data: What Abuse are We Looking For?' (2021) 44(2) *World Competition* 199-226 <<https://doi.org/10.54648/woco2021012>>.

²² Lindsey Barrett, 'Confiding in Con Men: US Privacy Law, The GDPR, and Information Fiduciaries' (2019) 42(3) *Seattle University Law Review* 1057-1113 <<https://digitalcommons.law.seattleu.edu/sulr/vol42/iss3/5/>>.

checks²³ or even ‘cyber abuses’ encountered in cybercrimes.²⁴ Nonetheless, recent abusive behaviours were equally identified from the data subject. After all these years of building the highly demanded user-centric legislation²⁵ that assigns the user ‘in the driver seat’,²⁶ this ‘dark side of rights’²⁷ becomes unsurprising: ‘If privacy and personal data protection point to over-emphasis on the individual and the personal in modern law, is there any alternative?’²⁸

The current version of the GDPR has no reference to abusive requests, but Article 12(5) can be interpreted for covering them. For now, Article 12(5) GDPR allows the limitation of manifestly unfounded or excessive requests through refusal of compliance, i.e. rejection, or payment of the administrative costs for complying with them. The interpretation of Dix underpinned that the ‘manifestly unfounded’ threshold is met ‘if even for an ordinary person it evidently exceeds the guaranteed rights of the data subject’, whereas ‘excessive’ ones were frequently understood through their repetitive character.²⁹ Following this, the abuse of right would seem to naturally fit within the former category, yet the Digital Omnibus took an opposite direction and linked it with excessiveness: ‘the excessive character of a request concerns the possibly abusive conduct of a data subject’ (para 35).³⁰

At the same time, the guidelines of the EDPB stressed that data controllers must interpret these concepts objectively and narrowly.³¹ However, the test indirectly extends to more subjective components, as ‘manifestly unfounded’ requests should be analysed through ‘the content and scope of the request’ (para 178), and ‘excessive’ requests through ‘malicious intent’ (para 190). As it will be shown, new developments officially coined an objective-subjective test for requests of access under the GDPR.

²³ Mariano Di Martino, Isaac Meers, Peter Quax, Ken Andries and Wim Lamotte, ‘Revisiting Identification Issues in GDPR “Right of Access” Policies: A Technical and Longitudinal Analysis’ (2022) 2022(2) *Proceedings on Privacy Enhancing Technologies* 95-113 <<https://doi.org/10.2478/popets-2022-0037>>.

²⁴ Gill Phillips, ‘The Abuse and Misuse of Technology’ (2016) 17(2) *Computer Law Review International* 43-51, 46 <<https://doi.org/10.9785/crl-2016-0203>>.

²⁵ Alex Bowyer, Jack Holt, Josephine Go Jefferies, Rob Wilson, David Kirk and Jan David Smeddinck, ‘Human-GDPR Interaction: Practical Experiences of Accessing Personal Data’ in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (ACM 2022) Article 106, 1-19 <<https://doi.org/10.1145/3491102.3501947>>.

²⁶ Bethany Sealey, ‘Has the 2016 General Data Protection Regulation Really Given Consumers More Control Over Their Personal Data?’ (2020) 1 *LJMU Student Law Journal* 17-41, 19 <<https://doi.org/10.24377/LJMU.SLJ.vol431rticle431>>.

²⁷ Gianluigi Palombella, ‘The Abuse of Rights and the Rule of Law’ in András Sajó (ed), *Abuse: The Dark Side of Fundamental Rights* (Eleven International Publishing 2006) 5-28, 6 <<http://dx.doi.org/10.2139/ssrn.992875>>.

²⁸ Susanna Lindroos-Hovinneimo, ‘Private Selves - An Analysis of Legal Individualism’ in Visa A J Kurki and Tomasz Pietrzykowski (eds), *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (Springer 2017) 29-46, 38 <https://doi.org/10.1007/978-3-319-53462-6_3>.

²⁹ Alexander Dix, ‘Art. 12: Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subjects’ in Indra Spiecker gen. Döhmman, Vagelis Papakonstantinou, Gerrit Hornung and Paul De Hert (eds), *General Data Protection Regulation: Article-by-Article Commentary* (C.H. Beck/Hart/Nomos 2023) 434-448, 445.

³⁰ European Commission (n 3).

³¹ EDPB (n 6).

In the *FT v DW* ruling,³² the data subject submitted a request of access to his dentist in Germany, with the intention to subsequently file a legal action for malpractice against him. Interestingly enough, in paras 31-32, the Court transposed the factual background into two major legal conclusions: (a) the ‘manifestly unfounded or excessive’ requests, as regulated in Article 12(5) GDPR, can be collectively referred to as ‘instances of abuses of rights’ and (b) the analysed request was not abusive, given that this was the first copy requested.

At the moment the decision was published, the implications were considerable, leading to a two-fold incongruity. Firstly, the view of the CJEU contradicted the view presented in the EDPB guidelines on the right of access,³³ which conflated solely excessive requests under the category of abusive requests, without the manifestly unfounded ones. Secondly, at a deeper level, the interpretation did not account for potential discrepancies identified at national level, where the transposition of the GDPR coined the abusive requests as a translation substitution for excessive requests. This is visible in Greece’s Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data.³⁴ Can there be a Greek abuse as both genus and species? Lastly, it appears that individuals could therefore submit requests of access, regardless of the underlying intention, simply because the legal provision that restricts the reasons for this right is part of a non-binding set of provisions, namely Recital 63 GDPR. As confirmed doctrinally, the GDPR does not link data protection rights to specific motivations, even if national courts may sometimes have opposing views, such as Germany.³⁵ This is why they were characterised as ‘intent-agnostic’ and ‘purpose-blind’.³⁶ The same applies to the United States too, where the Health Insurance Portability and Accountability Act of 1996 is applicable to patients accessing their medical records, without being limited to declare a purpose.³⁷

Furthermore, the *Österreichische Datenschutzbehörde v F R* case³⁸ shows that abusive intention and practices may be assessed as part of access requests submitted to data protection authorities too. Although the ruling examined the application of Article 57(4) GDPR, which mirrors Article 12(5) GDPR but does not form part of this contribution,³⁹ it explored the existence of abusive intention solely in conjunction with excessive requests (para 55). Without ruling out the adjacent category of ‘manifestly unfounded’ requests, the CJEU reiterated, at a generic level, that abusive requests are attached to excessiveness.

³² Case C-307/22 *FT v DW* [2023] ECLI:EU:C:2023:811.

³³ EDPB (n 6).

³⁴ Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data, Implementation of Regulation (EU) 2016/679, art 57(3) (Greece).

³⁵ Dominika Kuźnicka-Błaszowska, ‘Practitioners’ Corner: Excessive Use of Data Access Rights in the Practice of Imposing Administrative Fines’ (2024) 10(1) *European Data Protection Law Review* 105-110 <<https://doi.org/10.21552/edpl/2024/1/15>>.

³⁶ Jef Ausloos and Michael Veale, ‘Researching with Data Rights’ (2020) *Technology and Regulation* 136-157, 149 <<https://doi.org/10.26116/techreg.2020.010>>.

³⁷ Health Insurance Portability and Accountability Act of 1996, Pub L No 104-191, 110 Stat 1936.

³⁸ Case C-416/23 *Österreichische Datenschutzbehörde v F R* [2025] ECLI:EU:C:2025:3.

³⁹ See n 5 above.

Based on these observations, one should not confuse the abuse of right theory with the general prohibition against abusive use of EU law, officially established in the *Cussens and Others v Brosnan* case, after the CJEU's interpretation on the extensive case law on this matter.⁴⁰ Although both concepts were recognised as relevant in addressing the potential abuse of access rights,⁴¹ they have distinct values, as extensively outlined in the monograph of De la Feria and Vogenauer.⁴² The doctrine of abuse of right applies where individuals exercise legally conferred rights 'against their socio-economic function or to intentionally harm others', being narrower than a general prohibition against abusive practices, which is relevant even where no legal right exists, as exemplified in criminal law.⁴³ More precisely, abuse of law and abuse of right share an appearance of lawfulness, but differ in several respects, with the former involving the artificial acquisition of rights, whereas the latter concerning 'illegitimate exercises of existing rights'.⁴⁴ Given that this article analyses the limits of exercising the right of access conferred by Article 15 GDPR, it focuses on the doctrine of abuse of right.⁴⁵

2. *Ius Accessus et Abusus: Post Digital Omnibus*

Last year, the EC considered that the reasoning behind the varied forms of 'non-conformity' of data protection requests (by way of unfoundedness or excessiveness) calls for a review, in light of abusive requests (para 35).⁴⁶ This section will further explore the proposal's applicability and impact on data protection realms.

To begin with, this solution appears to contradict the interpretation of the CJEU. Simultaneously, it unjustifiably excludes any GDPR request that is not founded on Article 15 GDPR. For example, erasure requests, as regulated under Article 17 GDPR, were incorrectly not considered by the EC as potential routes for abusive requests. Although data protection rights beyond the right of access exceed the scope of this article, this point is notable for addressing potential gaps arising from the proposal and for suggesting future research directions. For example, the United Kingdom's Information Commissioner's Office (ICO) advised that multiple erasure requests intended to have an employee fired should be considered manifestly unfounded and rejected.⁴⁷ While this interpretation differs from the EU

⁴⁰ Case C-251/16 *Cussens and Others v Brosnan* [2017] ECLI:EU:C:2017:881.

⁴¹ Case C-526/24 *Brillen Rottler GmbH & Co. KG v TC* [2025] ECLI:EU:C:2025:723, Opinion of AG Szpunar, 18 September 2025.

⁴² Rita de la Feria and Stefan Vogenauer (eds), *Prohibition of Abuse of Law: A New General Principle of EU Law?* (Hart 2011).

⁴³ Dorota Leczykiewicz, 'Prohibition of Abusive Practices as a "General Principle" of EU Law' (2019) 56(3) *Common Market Law Review* 703-742, 735 <<https://doi.org/10.54648/COLA2019053>>.

⁴⁴ Alexandre Saydé, *Abuse of EU Law and Regulation of the Internal Market* (Hart 2014) ch 3, 28-30.

⁴⁵ A separate study may explore the broader framework and examine cases where the existence of the right itself is questionable, for example, as presented below, where a third party with no authority to act on behalf of the data subject attempts to commit a malware attack by submitting a malicious access request.

⁴⁶ European Commission (n 3).

⁴⁷ Information Commissioner's Office, 'Manifestly unfounded and excessive requests' (10 February 2023) <<https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/>> accessed 1 September 2026.

proposal's link to excessiveness and concerns law enforcement organisations, it suggests that abusive requests should not be limited to access rights.

On the other hand, the Digital Omnibus emphasises that the right of access is a benefit on the side of the data subject and its lawful exercise should be limited to intentions rooted in data protection (para 35). Examples to the contrary include the submission of requests with the sole intention of committing extortion, causing harm, damage or obtaining some sort of financial benefit, such as maliciously orchestrating the rejection of the request by the data controller and subsequently claiming compensation.

The most recent practical case illustrating the above-mentioned scenarios is *Brillen Rottler GmbH & Co. KG v TC*, in which two explicit refinements emerge: the recognition of abusive access requests,⁴⁸ and the direct application of abuse of right doctrine in the context of access rights.⁴⁹ In this case, the requester was considered to act abusively, although the right of access was exercised for the first time, because they developed a practice of subscribing to newsletters, and then claiming compensation. The abusive intention was inferred from an overarching examination, including the behaviour of the data subject. The Advocate General identified supplementary factors: 'the subject of the access request, the time that has elapsed between the consent to the processing and that request, the quantity and nature of the personal data covered by that request and the activity in the context of which it processes the data, if any' (para 54).⁵⁰

This case marked a significant turning point in the CJEU's approach to abusive data protection requests. First, it acknowledged that an objective-subjective test must be employed to determine the abusive character (para 36). Second, it provided unprecedented guidance on abusive intention, meaning 'where the data subject has made that request for a purpose other than that of being aware of the processing of those data and verifying the lawfulness of that processing, in order to be able, subsequently, to obtain protection of his or her rights under the GDPR' (para 40).

This recent jurisprudence departs from the *FT v DW* case⁵¹ on two points: it establishes that a request can be abusive even when it is submitted for the first time, and it ties abuse to excessiveness under Article 12(5) GDPR. On the first point, malicious intention weighs more heavily than the number of requests: as long as the data subject exhibits a behaviour in line with the law, they will be offered protection, irrespective of the specific intention. On the second point, it remains unclear whether abusive requests are a genus covering both 'manifestly unfounded or excessive requests', as previously implied, or a sub-species of one of them, as the *Brillen Rottler GmbH & Co. KG v TC* case⁵² outlines. An explicit position from the EU institutions would be welcome, although the distinction makes no

⁴⁸ Case C-526/24 *Brillen Rottler GmbH & Co. KG v TC* [2026] ECLI:EU:C:2026:216.

⁴⁹ *Brillen Rottler* (n 41) Opinion of AG.

⁵⁰ *ibid.*

⁵¹ *FT v DW* (n 32).

⁵² *Brillen Rottler* (n 48).

practical difference to this article, since the abuse-misuse dichotomy proposed below applies equally to both grounds under Article 12(5) GDPR, data controllers to refuse or charge the administrative costs for handling the request.

Nonetheless, the *Brillen Rottler GmbH & Co. KG v TC* case⁵³ emerged in the data protection world during the tumultuous times of the Digital Omnibus proposal, which similarly linked abusive requests to excessiveness, proposing a subjective component for assessing them. This shows more EU alignment. Previously, the dual test had limited visibility: in *Peter Nowak v Data Protection Commissioner* case,⁵⁴ only the Advocate General endorsed it.⁵⁵ In her interpretation, the subjective component was translated as ‘an undue advantage’ (para 44), found to be missing when the data subject exercised the right of access to their examination scripts, in absence of other routes of access. Thus, she not only concluded that no abuse occurred, but also confirmed that the use of the right of access was the sole means for obtaining access to the data lawfully.⁵⁶

Returning to the Digital Omnibus proposal, criticism was expressed by the European Data Protection Board and the European Data Protection Supervisor through their joint opinion (‘EDPB-EDPS joint opinion’), emphasising that the manifestly unfounded or excessive character of a request should be assessed in light of an objective test.⁵⁷ By exclusion, the subjective test was disregarded. However, they acknowledge in para 55 that the GDPR ‘should link the notion of ‘abusive requests’ with the existence of an abusive intention (e.g., evident intention to cause harm to the controller)’. In plain terms, requests of access could be considered abusive only when the intention behind it is abusive, as the abuse-misuse matrix proposed below will establish.

The new wording of Article 12(5) GDPR, as presented in the Digital Omnibus, allows the limitation of access requests ‘because the data subject abuses the rights conferred by this Regulation for purposes other than the protection of their data’.⁵⁸ However, one question remains: Should this be interpreted in the sense that more strictness is imposed and any scope that falls outside ‘pure’ data protection matters would constitute an abuse of the GDPR rights? The existing case law and doctrine weigh against such a reading, justifying the necessity for an interpretative framework.

Mahieu criticised the proposal, concluding that it acts against its purpose: it causes uncertainty, it breaches the Charter of Fundamental Rights of the EU and eventually, facilitates data controllers’

⁵³ *ibid.*

⁵⁴ Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994.

⁵⁵ Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:582, Opinion of AG Kokott, 20 July 2017.

⁵⁶ Although the interpretation provided by the Advocate General was expressed prior to the GDPR’s enforcement, its reasoning remains pertinent.

⁵⁷ European Data Protection Board and European Data Protection Supervisor, ‘Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)’ (2026) <https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_en> accessed 12 February 2026.

⁵⁸ European Commission (n 3) 56.

abuse.⁵⁹ The response of noyb - European Center for Digital Rights further strengthens these points, raising a substantial concern related to a violation of Article 8(2) of the Charter,⁶⁰ additionally voiced by the Dutch Council for Transport, Telecommunications and Energy.⁶¹ Paradoxically, the proposal was (and is) expected to still reflect the spirit of the law and the EU goals for harmonisation. Therefore, it ought to be understood as complementing previous international and EU legal instruments jointly with case law, unless explicitly permitted otherwise.

As a result, the proposal under the Digital Omnibus could still be reviewed, taking this criticism into account. Rather than reiterating potential flaws in yet another reformist contribution, this article will analyse the alternative routes: prohibiting data controllers from taking purpose into account for analysing access requests, as Rossi and others propose,⁶² or, accepting that purpose (or intention, as per the EDPB-EDPS joint opinion)⁶³ may exceptionally play a role and adopting an official interpretation of it, taking into account both businesses and data subjects. The following section will pursue the latter, provided that the Digital Omnibus is adopted as currently written, and any procedural deficiencies that would otherwise make it incompatible with EU legislation, such as a detailed impact assessment,⁶⁴ are resolved. A categorical ban on data controllers examining the intention behind a request cannot be accepted as it artificially compels them to tolerate illegitimate behaviour. Such a one-sided framework consequently tips the balance entirely towards protecting data subjects from potential abuse by data controllers, while granting no corresponding protection against abuse by data subjects.

III. Access at the Crossroads of Abuse and Misuse

It is agreed that the *ius accessus* was primarily designed for enabling data subjects to ‘be aware of, and verify, the lawfulness of the processing’ as per Recital 63 GDPR. Hence, using this tool for other motives would fall outside what was envisaged by the legislator. However, this does not imply that the intention or the overall conduct would be automatically unlawful or malicious. In reality, access requests could also serve as a powerful instrument for supporting other legal rights, as it will be detailed below. This is substantiated by the EDPB-EDPS joint opinion on the Digital Omnibus (para 54).⁶⁵ Therefore,

⁵⁹ René Mahieu, ‘The Ominous Omnibus: Dismantling the Right of Access to Personal Data’ (Verfassungsblog, 3 December 2025) <<https://verfassungsblog.de/digital-omnibus-right-of-access-to-personal-data/>> accessed 13 June 2026.

⁶⁰ noyb - European Center for Digital Rights, ‘Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the Commission (Version 3)’ (24 February 2026) <<https://noyb.eu/en/digital-omnibus-report-v3-analysis-select-gdpr-and-eprivacy-proposals-commission>> accessed 11 June 2026.

⁶¹ Council for Transport, Telecommunications and Energy, ‘Verslag van een schriftelijk overleg’ (20 April 2026) Tweede Kamer, 2025–26, 21 501-33, no 1195, 8.

⁶² Julien Rossi, Jonathan Keller, Nawale Lamrini, René Mahieu and Jessica Pidoux, ‘DATARights Policy Brief on Data Subject Access Rights in the Proposed Digital Omnibus’ (2026) *CEMTI, Université Paris 8* <<https://hal.science/hal-05545314v1/document>> accessed 1 August 2026.

⁶³ EDPB and EDPS (n 57).

⁶⁴ *ibid.*

⁶⁵ *ibid.*

this caveat could be encapsulated in distinction between the legitimate or illegitimate manner of exercising access rights, corresponding to abuse and misuse respectively.

With a progressive, solution-oriented outlook, this section proposes an interpretation that sharpens the GDPR's application, at no additional regulatory costs. At a macro (conceptual) level, the distinction between abuse and misuse could complement the restriction of exercising the right of access abusively, and, at a micro (EU regulatory) level, the proposal for amending Article 12(5) GDPR could still be successful without contradicting the previous EU acquis. In this sense, the EDPB already implied that there would be a difference between these two concepts in the context of access requests, despite the lack of further explanations: 'controllers may fear that granting access could expose their organisation to abuse or misuse'.⁶⁶

Comparatively, a delineation between abuse and misuse was already suggested in the UK, with respect to vexatious requests⁶⁷ under freedom of information legislation, which protects a related right of access.⁶⁸ Furthermore, the legal branch of intellectual property, which was oftentimes analysed together with data protection, although not being fully overlapped,⁶⁹ may have refined the groundwork for this distinction. In Hilty's examination on 'dysfunctional uses or conduct' in intellectual property rights, it was recognised that misusing a right is a narrower and less frequent concept than abuse.⁷⁰ Even if the concepts are sometimes used inaccurately in legislation, the same author defined misuse as the 'improper, inappropriate, incorrect use of something, divergent from its intended use (or understanding)', while acknowledging that abuse originates from a more negative angle, relying on 'deliberate intention'.⁷¹ Similarly, a later study in this field added that misuse and abuse should be understood as opposing poles of an axis, with multiple grey areas in the middle: 'the targeted conducts can be classified along a spectrum that ranges from rare cases of pure abuse, which entail the wilful causation of damages to others, to different shades of misuse, darker or lighter depending on the degree of departure of the behaviour from the function(s) of the right exercised, the reasons why it has been conferred, and the interest it is meant to protect'.⁷²

⁶⁶ European Data Protection Board, '2024 Coordinated Enforcement Action: Implementation of the Right of Access by Controllers' (16 January 2025) 23 <https://www.edpb.europa.eu/system/files/2025-01/edpb_cef-report-2024_20250116_rightofaccess_en.pdf> accessed 12 June 2026.

⁶⁷ Information Commissioner's Office, 'Dealing with vexatious requests' (1 August 2023, section 14) <<https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/section-14-dealing-with-vexatious-requests/>> accessed 22 June 2026.

⁶⁸ Freedom of Information Act 2000.

⁶⁹ Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193-220 <<https://www.jstor.org/stable/1321160>> accessed 25 June 2026; Pamela Samuelson, 'Privacy As Intellectual Property?' (2000) 52(5) *Stanford Law Review* 1125-1173 <<https://doi.org/10.2307/1229511>> accessed 25 June 2026.

⁷⁰ Reto M Hilty, 'Legal Remedies Against Abuse, Misuse, and Other Forms of Inappropriate Conduct of IP Right Holders' in Reto M Hilty and Kung-Chung Liu (eds), *Compulsory Licensing: Practical Experiences and Ways Forward* (Springer 2015) 377-396 <https://link.springer.com/chapter/10.1007/978-3-642-54704-1_18>.

⁷¹ *ibid* 380.

⁷² Caterina Sganga and Silvia Scalzini, 'From Abuse of Right to European Copyright Misuse: A New Doctrine for EU Copyright Law' (2017) 48 *International Review of Intellectual Property and Competition Law* 405-435, 425 <<https://doi.org/10.1007/s40319-017-0584-z>>.

In order to apply the abuse-misuse distinction to the right of access it is crucial to establish what abuse of right means in general. Historically, it was recognised that abuse of rights can occur in two situations: (a) when there is no underlying interest, and (b) when interest exists, but it is illegitimate.⁷³ This was confirmed in most civil law systems that recognise the abuse of right theory, defining it as: one party ‘...obtains little or no benefit from the exercise of his rights while, at the same time, the other party or parties suffer damages thereby’.⁷⁴ However, the mere result of harm on the counterpart does not automatically result in such abuse: the critical element is the legitimacy behind the exercise, which comes as an application of the *neminem laedit qui suo jure utitur* (one who exercises their legal rights harms no one) principle.⁷⁵ The criterion of legitimacy, inspired by the compatibility of the right of access ‘with the objectives of the provision enshrining it’,⁷⁶ will guide the following analysis.

On this basis, a legitimate use of the right of access for a purpose beyond data protection shall be considered misuse. It should be noted that this use of the term carries no negative connotation, even though, on the data controller’s side, misuse of personal data practices identified in recent years has typically been associated with the opposite: price discrimination, privacy violations, location-based steering, and combinations thereof.⁷⁷

Although the misuse of the right of access to personal data is a rather absent topic in doctrine, Ausloos and Veale confirm the ‘misuse’ of access rights as a legitimate practice, opposed to an abuse of rights. Precisely, in their study, research as an access request purpose was concluded to be unlikely to fall within the latter, while being recognised as amounting ‘to misuse/retrofit a legal device for unintended purposes’.⁷⁸ Comparatively, in cyber-security, Trojan Horses⁷⁹ were also classified as legitimate and illegitimate.⁸⁰ Their way of operation is unchanged, but the difference comes from how they are used: the former serve lawful reasons, such as police investigations,⁸¹ while the latter rely on malicious motive.

⁷³ Gutteridge (n 17).

⁷⁴ Julio Cueto-Rua, ‘Abuse of Rights’ (1975) 35 *Louisiana Law Review* 965-1013, 991 <<https://digitalcommons.law.lsu.edu/lalrev/vol35/iss5/3>>.

⁷⁵ Jossierand (n 19).

⁷⁶ *Brillen Rottler* (n 41) Opinion of AG.

⁷⁷ Cihat Börklüce, ‘Big Data Misuse and European Contract Law’ (2024) 20(4) *European Review of Contract Law* 320-347 <<https://doi.org/10.1515/ercl-2024-2012>>. However, this author occasionally uses the term ‘abuse’ in a manner that may confusingly imply an overlap between these concepts.

⁷⁸ Ausloos and Veale (n 36) 149.

⁷⁹ Trojan Horse can be defined as ‘a program that appears as a useful and harmless, and once it has been installed in a victim computer, it begins to carry out malicious acts such as stealing important information from victim’s computer’ as per Areej Mustafa Abuzaid, Madihah Mohd Saudi, Bachok M Taib and Zul Hilmi Abdullah, ‘An Efficient Trojan Horse Classification (ETC)’ (2013) 10(2) *International Journal of Computer Science Issues* 96-104 <<https://scispace.com/pdf/an-efficient-trojan-horse-classification-etc-2gdp546g9r.pdf>>.

⁸⁰ Golden G Richard, Andrew Case, Modhuparna Manna, Elsa A M Hahne and Aisha Ali-Gombe, ‘Digital Investigation and the Trojan Defense, Revisited’ in Anthony C Ijeh and Kevin Curran (eds), *Crime Science and Digital Forensics: A Holistic View* (CRC Press 2021) 67-84 <<https://doi.org/10.1201/9780429322877>>.

⁸¹ Eldar Haber, ‘The Law of the Trojan Horse’ (2024) 57 *UC Davis Law Review* 1667-1720 <<https://ssrn.com/abstract=4400283>>.

A new opportunity for cyber-attackers arises through access requests, functioning as entry points, which, once compromised, may successfully result in the intended harm. Such a case could hypothetically occur if the data subject exercises their access rights under Article 15 GDPR and attaches malware disguising it as the file containing additional details for the request, whether in an online or offline environment.⁸² In this situation, the right exists but is exercised maliciously, amounting to an abusive request. While criminal liability arising from such an act is not excluded,⁸³ this research remains focused on the GDPR, Regulation which does not form part of criminal law but may contribute to its application.⁸⁴ Accordingly, the data controller would most likely still be expected to formally respond to the request, as per Article 12(3) GDPR: ‘The controller shall provide information on action taken on a request (...)’. Contrastingly, if the requester were an unauthorised third party attaching malware to an access request, no right would exist, and the obligation would fall away, rendering the misuse-abuse distinction redundant.⁸⁵ Essentially, even identity checks could, hypothetically, have malware files or links attached to the documents submitted for verification, as in the case of diplomats who were targeted by a malware attached to pictures of the vehicle they considered buying.⁸⁶

Doctrinally, examples of what was referred to as ‘adversarial SAR’ can range from any type of ‘focused’ harm (e.g. to ensure the business has less resources to allocate on other projects that are known to the requester, to use it purely as a revenge mechanism for any situation which previously created frustration to the requester) or less ‘focused’ (e.g. to simply cause disruptions or distractions).⁸⁷ Ultimately, financial loss may occur. The intention is unequivocally malicious, as exemplified above, and qualifies as abusive in line with the joint EDPB-EDPS joint opinion on the Digital Omnibus.⁸⁸

On the other side of the spectrum, where the right of access is exercised with any intention other than to (generally) cause harm, but still outside the realms of data protection, the behaviour would fall

⁸² With the caveat that an offline data subject access request could hide a malware attack only if some digital component is attached to it. For instance, the request may be printed and delivered to the data controller, but accompanied by a link or external storage device connecting to the controller’s system, purportedly containing further details or identification information, thereby triggering the virus infection. This nuance follows from the fact that malware is ‘software designed with a nefarious intent of harming the computer user’, as per Fawn T Ngo and others, ‘Malicious Software Threats’ in Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Palgrave Macmillan 2020) 793-813 <https://doi.org/10.1007/978-3-319-78440-3_35>.

⁸³ The attacker from this example could be subject to the national implementation laws of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8, which explicitly frames ‘criminal law responses to cybercrime’ within its stated goals (Recital 2).

⁸⁴ David Wicki-Birchler, ‘The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?’ (2020) 1 International Cybersecurity Law Review 63-72, 71: ‘The fight against cybercrime was not the primary goal of GDPR, but rigorous implementation of the above-mentioned security measures would significantly contribute to the efficient containment of criminal activity in the Internet.’

⁸⁵ On why this topic may be of interest for future research, see n 45 above.

⁸⁶ Pierluigi Paganini, ‘Russia-Linked APT Used a Car for Sale as a Phishing Lure to Target Diplomats with HeadLace Malware’ (*Security Affairs*, 3 August 2024) <<https://securityaffairs.com/166496/apt/russia-apt-headlace-malware.html>> accessed 20 March 2026.

⁸⁷ Di Martino and others (n 23).

⁸⁸ EDPB and EDPS (n 57).

under the concept of misuse. To exemplify, research, credit scoring and online casino engagement were equally recognised as legitimate purposes of access requests in the report issued by noyb - European Center for Digital Rights as a response to the Digital Omnibus proposal.⁸⁹ This would also be the case for using the right of access as a ‘pre-litigation tool’, progressively observed across various jurisdictions, including Belgium, France, Germany, Ireland, the Netherlands,⁹⁰ and the UK.⁹¹ Coming back to the *FT v DW* case,⁹² if someone used the right of access as an evidence-gathering ‘weapon’ in malpractice litigation, the request would still fall within the law. Indirectly, that can still harm the reputation or even the finances of the medical professional in question, but essentially, the patient would be exercising all rights within the limits of the law. As concluded by the CJEU, that request was not an instance of abuse of right and should have been complied with.

However, real-life scenarios are not always following a black and white matrix. As the article of Sganga and Scalzini detailed in the field of intellectual property abuse and misuse, multiple cases may fall in the middle.⁹³ In data protection, an example may be when former partners who have undergone divorce are looking into current information about their counterparty.⁹⁴ In this case, a two-fold response is needed. At intention level, if the former partner is collecting evidence for exercising another legal right (e.g. due to a breach of the previous divorce settlement), the request of access should be generally complied with, as a misuse of right. Nonetheless, the opposite applies if the former partner acts with the intention to harass the counterparty, thereby rendering the request abusive. In this second case, such a request could be rejected also for the lack of authorisation to act on behalf of the counterparty, following the EDPB guidelines on the right of access.⁹⁵ Practically, however, data controllers often fail to conduct these checks correctly, as extensively exemplified by studies in which access requests are impersonated using lookalike email addresses.⁹⁶

⁸⁹ noyb (n 60).

⁹⁰ Marga Caproni, Chelsea Gunning and Malgorzata Grzelak, ‘ECJ Ruling on Data Subject Access Requests: Some Welcome Relief for European Employers, or not quite yet? (Part II)’ (Employment Law Worldview, 28 May 2026) *Employment Law Worldview* <<https://www.employmentlawworldview.com/ecj-ruling-on-data-subject-access-requests-some-welcome-relief-for-european-employers-or-not-quite-yet-part-ii/>> accessed 22 June 2026.

⁹¹ *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74.

⁹² *FT v DW* (n 32).

⁹³ Sganga and Scalzini (n 72).

⁹⁴ Di Martino and others (n 23).

⁹⁵ EDPB (n 6).

⁹⁶ Di Martino and others (n 23); Mariano Di Martino and Others, ‘Personal Information Leakage by Abusing the GDPR “Right of Access”’ in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (USENIX Association 2019) 371-386 <https://www.usenix.org/system/files/soups2019-di_martino.pdf>; Matteo Cagnazzo, Thorsten Holz and Norbert Pohlmann, ‘GDPiRated – Stealing Personal Information On- and Offline’ in Kazuo Sako, Steve Schneider and Peter YA Ryan (eds), *Computer Security – ESORICS 2019* (Springer 2019) 367-386 <https://doi.org/10.1007/978-3-030-29962-0_18>; Luca Bufalieri and others, ‘GDPR: When the Right to Access Personal Data Becomes a Threat’ in *2020 IEEE International Conference on Web Services (ICWS)* (IEEE 2020) 75-83 <<https://doi.org/10.1109/ICWS49710.2020.00017>>; James Pavur and Casey Knerr, ‘GDPArrrrr: Using Privacy Laws to Steal Identities’ (Black Hat USA, Las Vegas August 2019) <<https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>> accessed 20 September 2026.

Beyond binary scenarios, the intention behind the act may also be mixed, in which case the prevailing intention will dictate the outcome: if that is related to harm or malice, then the conduct cannot be excused or protected, additionally triggering liability.⁹⁷ The fact that the requester may be interested in research, while covertly attaching malware to their access request, would not negate the abuse.

The abuse-misuse distinction should not result in a system that would expose data subjects to the abuse of data controllers. The examination of the data subject access request should remain as narrow as necessary to establish the existence or absence of legitimacy, while remaining as generic as necessary to preserve the data subject's freedom to submit the request. Therefore, data controllers would be expected to take a holistic view of the elements attached to the request in order to determine whether it may be abusive, without imposing an obligation on the data subject to specify a purpose for submission.

As a result, two effects emerge. First, the abuse-misuse framework rests on the presumption that access requests are to be treated as a misuse of right where the intention behind them is unrelated to data protection, unless the controller identifies illegitimate intention. Similarly, the EU regime in copyright misuse was considered as a generic and residual tool for conduct that is not regulated otherwise.⁹⁸ Second, the burden-of-proof rule set out in Article 12(5) GDPR remains untouched. Abuse cannot be assumed. Hence, the controller is responsible for justifying a finding of abuse of the right and the application of the exceptional mechanisms under Article 12(5) GDPR. In this manner, the concern raised by the Dutch Council for Transport, Telecommunications and Energy, that the Digital Omnibus could make the data subjects responsible for proving that their request concerns data protection, is avoided,⁹⁹ at no additional regulatory costs.

The legitimacy criterion underlying the proposed abuse-misuse distinction could therefore enable controllers to rely on the exceptional mechanisms in Article 12(5) GDPR to restrict the abusive exercise of the right of access, while allowing requests with a legitimate non-data-protection intention, such as the common practice of evidence-gathering. These legitimate requests would generally be excluded from the applicability of this provision, unless other criteria (such as repetitiveness) apply. In this way, the Digital Omnibus' proposed limitation on the abuse of the right of access 'for purposes other than the protection of personal data' (para 35) could still stand, without creating uncertainty for either data controllers or data subjects.

⁹⁷ Josserand (n 19), metaphorically noting that a handful of good grains cannot have the capacity to purify weeds.

⁹⁸ Sganga and Scalzini (n 72).

⁹⁹ Council for Transport, Telecommunications and Energy (n 61).

IV. Conclusive Remarks

EU data protection is currently undergoing major re-evaluation debates. This novel wave of reviews comes with a proposal that targets most of the regulations impacting the digital world. For the GDPR, given its historic success, extraterritorial effect and global footprint, the repercussions are even more significant. As a result, the coming months are expected to place substantial emphasis on understanding and synchronising the proposal within the broader regulatory ecosystem. This task already proves particularly challenging, considering the criticism concerning a potential breach of the Charter of Fundamental Rights of the European Union and the divergence from CJEU case law.

In this context, data controllers must be aware of the legal avenues at their disposal. As illustrated, doctrine and case law abound in examples where medical law, employment law, or family law were associated with a ‘weaponised’ use of the right of access under Article 15 GDPR, without being abusive. Hence, a more precise set of rules is needed, capable of being easily understood and applied through real-life cases. If the Digital Omnibus proposal is to be understood as a definitive panacea, abusing the right of access becomes a land of entangled interpretations, where the EDPS and EDPB become actors with a salvational role.

By magnifying and dissecting all angles related to the proposal on limiting abusive access requests, this article explored the route of splitting the non-data-protection-related exercise of the right of access into abuse and misuse of the right. The core criterion for doing so was set as the legitimacy behind the request, underscoring the absence of a prerequisite from the data subject to provide precise explanations. In this way, clear, fair and balanced solutions can be provided to requests rooted in extraneous motivations, while securing EU legal coherence and data subjects’ protection. This approach facilitates reconciliation, following the proposed objective-subjective test for abusive requests, without increasing regulatory costs.

Data subject access requests will continue to be used for various reasons, which should not in themselves be regarded as problematic. Fundamental rights deserve adequate protection. Nonetheless, the malicious motives attached to innocently looking requests, taking shapes like deception, animosity, and grievance, cannot be disregarded. As a result, the current article proposed an interpretative model which builds upon the existing legal corpus from the abuse of right doctrine and intellectual property scholarship, allowing data controllers to act against abusive exercises of access rights. Eventually, this approach seeks to reduce both the risk of harm and unnecessary resource expenditure.