Judicial Uncertainties and Current Issues in the Compensation of Non-Material Damages under Article 82 GDPR

Güliz Arpalı *
**LL.M. graduate (German Law), University of Munster, Germany. For correspondence: garpali@uni-muenster.de, arpalıguliz@gmail.com.*

Digitalisation has turned personal data infringements into a problem area that directly affects individuals' personality-related interests and fundamental rights. Although Article 82 GDPR provides compensation for both material and non-material damage, the infringement–damage distinction especially for non-material harm and the scope of compensable claims remain contested. After Österreichische Post rejected a minimum seriousness threshold, the post-threshold challenge is to draw a workable boundary between ordinary inconvenience and compensable adverse effects without sliding into automatic compensation. This article proposes a two-step standard for substantiating harm in fear/anxiety and loss-of-control claims, aiming to objectify the assessment of non-material damage. It further develops an evidentiary architecture that connects Article 5(2) GDPR accountability with the secondary burden of substantiation to counterbalance information asymmetries in digital disputes. Finally, it examines quantification and the place of non-monetary redress particularly apologies in the PTAC line under the requirement of full and effective compensation.

Keywords: Article 82 GDPR; non-material damage; loss of control; fear/anxiety; burden of proof; accountability; secondary burden of substantiation; compensatory principle.

I. Introduction

In the digital age, personal data have become a source of value and power that directly shapes individuals' identities, private lives, and fundamental rights. As data processing through social media, big data analytics, and cloud technologies has become an ordinary feature of everyday life, the protection of personal data has moved beyond a narrow debate about technical compliance and has become a fundamental-rights-oriented issue that touches the individual's sphere of personality. One of the most significant private-law manifestations of this transformation is the compensation mechanism laid down in The General Data Protection Regulation (GDPR) Article 82, which enables individuals who have suffered harm as a result of unlawful processing to seek redress for their material or non-material damage.[1]

The practical effectiveness of Article 82 nevertheless depends on an ongoing debate over what counts as non-material damage and under which conditions it is compensable. A key turning point is Österreichische Post, where the Court of Justice of the European Union (CJEU) rejected national-law restrictions that make compensation contingent on a minimum seriousness threshold and affirmed non-material damage as an autonomous concept of EU law. In the post-threshold phase, the central question is how to draw a workable boundary between damage and mere inconvenience, and how claimants under conditions of digital information asymmetry can substantiate harm before courts through appropriate evidentiary means. The core tension is between ensuring effective redress in line with the GDPR's high level of protection and preventing a mere infringement from automatically translating into compensation.[2] Within this framework, three "persistent challenges" can be distinguished. The first is definitional: how the autonomous EU-law concept of "damage" should be given substantive content, and which criteria allow fear and loss of control to be distinguished from everyday inconvenience and qualified as compensable non-material harm. The second is evidentiary: how to construct the infringement–damage–causation nexus in the face of

[1] Art 82(1) GDPR; See Also Recital 146 GDPR.
[2] Case C-300/21 UI v Österreichische Post AG EU:C:2023:370, para 51.

asymmetries produced by the digital context, and how the controller's accountability role affects evidentiary burdens. The third concerns quantification and forms of redress: which criteria should govern the amount of compensation, and how non-monetary remedies most notably an apology in the PTAC line relate to the standard of full and effective compensation. Against this background, the article adopts a doctrinal method and examines recent CJEU case law as an analytically coherent body. It first develops workable criteria to maintain the infringement–damage distinction within the autonomous definition of damage. It then turns to evidentiary architecture, assessing the controller's role under Article 5(2) GDPR and the potential and limits of the secondary burden of substantiation as a procedural counterbalance. Finally, it analyses quantification and symbolic forms of redress in light of the compensatory principle, and proposes a coherent framework aimed at reducing uncertainties faced by national courts, particularly regarding proof and the determination of compensation.

II. The Autonomous Nature of Damage Under Article 82 and the Definition Problem

1. The "Autonomous" Character of Damage and the Detachment from National Law

For liability to arise under Article 82 GDPR, the claimant must establish not only an infringement and a causal link, but also the existence of damage. Damage may be either material or non-material. In the GDPR context, non-material damage captures adverse effects emotional, psychological, or social that result from an interference with an individual's personality rights, privacy, or psychological integrity.[3] However, the absence of a positive definition of non-material damage in Article 82 GDPR keeps alive the risk that the concept of damage will be filled by reverting to entrenched national damage doctrines. That risk may lead the same type of GDPR infringement to produce different outcomes across Member States and may undermine the GDPR's claim to provide uniform protection at Union level. For this reason, the concept of non-material damage must not be treated as a category that can be narrowed through national criteria; rather, it must be interpreted as an autonomous concept of EU law in light of the Regulation's objectives and systematic structure.[4] Indeed, in its request for a preliminary ruling in VI ZR 258/24, the German Federal Court of Justice (BGH) stated that because Article 82(1) contains no reference back to national law the concept of non-material damage must be defined as an autonomous concept of EU law. It further stressed that, in light of Recital 146, this concept must be interpreted broadly and must not be made subject to national threshold requirements.[5] Recital 146 indicates that the EU legislature deliberately refrained from introducing a narrowly restrictive approach and instead sought to assess damage from a broad perspective in order to safeguard the protection of personal data. This expansive textual framework is reinforced in particular by the explicit wording of Recital 146, which directly refers to the principle of full and effective compensation. It emphasises that such compensation should cover not only material loss but also non-material harm that may arise from interferences with personality rights.[6]

At the same time, an autonomous interpretation does not entail an infringement = automatic compensation outcome. As the BGH emphasised relying on CJEU case law in its request for a preliminary ruling in VI ZR 258/24, a mere infringement of the GDPR, taken in isolation, does not give rise to a right to damages. Under Article 82, it remains necessary that material or non-material damage has occurred and that a causal link is established between that damage and

---

[3] Ondřej Pavelek and Hana Adamová, 'Court of Justice of the European Union on Non-material Damage' (2022) 30 Časopis pro právní vědu a praxi 547.

[4] *Niklas Kerschbaumer-Gugu, Schadenersatz bei Datenschutzverletzungen: Die Haftung für Datenschutzverletzungen nach Art 82 DSGVO, § 29 DSG und ABGB* (Verlag Österreich 2019) 67, 73.

[5] Bundesgerichtshof (BGH), Beschluss vom 28 August 2025 - VI ZR 258/24, ECLI:DE:BGH:2025:280825BVIZR258.24.0, para 47.

[6] *Lea Stegemann, Der immaterielle Schadensersatz bei Datenschutzverstößen* (Nomos 2024) 110–113.

the infringement.[7] Accordingly, an autonomous interpretation, while curbing categorical national exclusions of a *de minimis* type, also requires that the infringement–damage–causation distinction be applied in each case through a context-sensitive, reasoned, and objectively verifiable assessment.[8]
The autonomous concept of damage also becomes apparent in the tension it creates with national procedural autonomy: while Member States retain discretion over procedural details, that discretion may not be exercised in a manner that weakens the GDPR's effectiveness (*effet utile*).[9]

2. Typology of Non-Material Damage: Fear/Anxiety, Loss of Control, and Reputational Harm
Although the GDPR does not provide a general definition of non-material damage under Article 82, the CJEU's case law suggests that it is possible to structure the concept into sub-categories such as emotional distress and stress, loss of control, and reputational harm.
Fear[10] and stress[11] are among the most frequently invoked and most contested components of non-material damage under the GDPR. They encompass adverse psychological effects triggered by a data breach, such as fear, anxiety, unease, anger, or an erosion of trust. Compensation for non-material damage is intended to redress not only economic loss but also these impacts on an individual's psychological integrity. [12]
In Wien Energie / Natsionalna agentsia za prihodite , the CJEU accepted that the anxiety and worry experienced by individuals affected by a personal data breach arising from the possibility that their data may be misused can fall within the scope of non-material damage. The Court emphasised that the fact that the data have not (yet) been actually misused does not negate these emotional effects, and that even the perception of a potential risk may amount to a genuine non-material harm.[13] Similarly, in Österreichische Post , the Court emphasised that even the slightest feelings of unease, discomfort, anxiety, or loss of trust may fall within the concept of damage. This makes clear that compensation is not confined to serious infringements or severe non-material effects: even minimal adverse impacts that an individual can concretely experience in everyday life may, in principle, found a claim for damages. The approach thus confirms that non-material damage cannot be made subject to a minimum threshold; rather, any perceptible adverse effect arising from a personal data infringement must be capable, in principle, of being brought within the concept of damage.[14]
Loss of control refers to the uncertainty and sense of insecurity that arise when an individual can no longer exercise agency over their personal data and does not know by whom, and for what purposes, the data are being processed. This phenomenon does not merely generate a feeling of discomfort or unease; it also entails a direct interference with the very core of the right to the protection of personal data namely, effective access to information and the freedom to exercise control over one's data.[15] Recital 75 provides an important anchor at this point. It

[7] BGH (n 5) para 13.
[8] UI v Österreichische Post (n 2) para 42.; Case C-741/21 *GP v juris GmbH* EU:C:2024:288, para 34.; Case C-590/22 AT and BT v PS GbR and Others EU:C:2024:536, para 25.
[9] Claudio Aliprandi, Datenschutzrechtlicher Schadensersatz nach Art. 82 DS-GVO: Voraussetzungen, Rechtsfolgen und Praxisbezüge (Nomos 2023) 260–62.
[10] OLG Koblenz, Urteil vom 18 May 2022 – 5 U 2141/21, BeckRS 2022, 11126, para 68.; Roman Dickmann, 'Nach dem Datenabfluss: Schadenersatz nach Art. 82 der Datenschutz-Grundverordnung und die Rechte des Betroffenen an seinen personenbezogenen Daten' (2018) *r+s*, 345.
[11] OLG Köln, Urteil vom 14 July 2022 – 15 U 137/21, NJW-RR 2023, 564, para 15.; AG Pfaffenhofen a.d. Ilm, Urteil vom 9 September 2021 – 2 C 133/21, BeckRS 2021, 27106.
[12] Matthias Bergt, 'Art 82 DS-GVO' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung / Bundesdatenschutzgesetz: DS-GVO / BDSG* (3rd edn, C H Beck 2020) para 18a (B).
[13] Case C-340/21 VB v Natsionalna agentsia za prihodite EU:C:2023:986, para 86.
[14] Oberster Gerichtshof (OGH) (Austria), Beschluss vom 15 April 2021 – 6 Ob 35/21x, para 21.
[15] Bergt (n 12) para 18b.

makes clear that the risks arising from the processing of personal data are not limited to economic or physical consequences, but also include situations that have a direct impact on individuals' fundamental rights and freedoms. In particular, it explicitly lists scenarios in which data subjects are deprived of their rights and freedoms in relation to their personal data or lose control over their personal data as among the envisaged types of harm/risk.[16]

The CJEU's statement in Scalable Capital that there is no hierarchy between categories of damage indicates that, in principle, a loss of control may be considered within the scope of compensable harm. At the same time, the Court also noted in that judgment particularly in the context of identity theft the relevance of whether personal data were actually misused.[17] This judgment suggests that a distinction must be drawn between an abstract loss of control and a risk that can be objectively substantiated. The literature likewise argues that loss of control approaches the category of compensable harm only insofar as it is linked to a concrete risk or effect impacting protected fundamental-rights interests, and emphasises that the notion of risk should not be expanded without limits.[18]

Reputational impairment is often the most visible external manifestation of a loss of control over personal data. Making inaccurate, outdated, or sensitive data accessible to third parties can lead to a loss of trust in an individual's social environment, diminished standing in business relationships, or harm to professional reputation. Such infringements affect not only an individual's psychological integrity but may also have direct consequences for their economic and professional life. For instance, the disclosure of erroneous financial data may negatively affect a person's creditworthiness, while the exposure of health data may weaken an individual's position in the labour market.[19] For example, in ArbG Dresden, the court accepted that the unauthorised disclosure of health data to third parties undermined the data subject's social standing and led to a loss of trust within their professional environment. The court found that the uncontrolled dissemination of such sensitive data can have direct adverse effects on an individual's reputation and, on that basis, treated the resulting reputational harm as non-material damage and awarded compensation to the claimant.[20]

In conclusion, the sub-categories of non-material damage commonly discussed under Article 82 GDPR emotional distress, loss of control, and reputational impairment directly affect both an individual's subjective psychological integrity and their position in social and professional life. The presence of these harms is not confined to an internal sense of unease and uncertainty; it may also produce outward-facing consequences, such as loss of trust, diminished standing, and strain in social relationships. Non-material damage thus forms an integral part of the GDPR's high level of protection, aiming to ensure the effective safeguarding of personality rights independently of economic loss.

3. The Post-Threshold Question: How Should the Boundary Be Drawn?

The CJEU's scepticism towards a minimum harm threshold constrains national exclusionary filters of a *de minimis* type,[21] but it simultaneously brings another risk into sharper focus: the

---

[16] GDPR recital 75.

[17] Joined Cases C-182/22 and C-189/22 JU and SO v Scalable Capital GmbH (Scalable Capital) EU:C:2024:531, para 42.

[18] Stephan Mulders, 'Risk and fundamental rights infringements as a form of "damage" per Article 82 GDPR' (*International Data Privacy Law*, published 8 December 2025) 5 https://doi.org/10.1093/idpl/ipaf030 accessed 23 February 2026.

[19] GDPR recital 75,85.; ürgen Taeger and Detlev Gabel (eds), DSGVO – BDSG – TTDSG (4th edn, Fachmedien Recht und Wirtschaft in Deutscher Fachverlag GmbH 2022), para 31.; Oberster Gerichtshof (OGH) (Austria), Beschluss vom 15 April 2021 – 6 Ob 35/21x,; Case C-687/21 BL v MediaMarktSaturn Hagen-Iserlohn GmbH EU:C:2024:72.

[20] ArbG Dresden, Urteil vom 26 August 2020 – 13 Ca 1046/20 (juris) para 5.

[21] VB v Natsionalna agentsia za prihodite (n 13), para 86.; UI v Österreichische Post (n 2) para 51 f.

collapse of the distinction between infringement and damage. For that reason, the core of the post-threshold debate is less the question of whether a harm threshold exists and more how to preserve the doctrinal distance between infringement and damage. Otherwise, Article 82 risks ceasing to operate as a compensatory regime and drifting towards an infringement → compensation automatism.[22]

The solution at this stage is not to impose an abstract "intensity" threshold, but to clarify the standard for substantiating harm. Particularly in claims based on fear/anxiety and loss of control, the assessment of harm can be objectified in two steps: (i) demonstrating, in light of the protective logic of Articles 7 and 8 of the Charter, the specific rights- or interest-domain in which the alleged adverse effect materialises; and (ii) identifying case-specific grounds that distinguish this adverse effect from the general risk perceptions of everyday life. This introduces an analytical intermediate layer between a mere statement of feelings and a compensable outcome.[23]

The second axis concerns risk-based claims. In data breach cases, harm often stems not from proven misuse that has already occurred, but from unease and uncertainty driven by forward-looking risks. However, for risk to serve as a basis for compensation, it must be taken beyond an abstract possibility that could be asserted in any infringement and concretised in light of the specific circumstances of the case.[24] In practice, this concretisation can be achieved by reference to the nature and context of the data (its sensitivity and privacy intensity), the circle of access (who had access and how widely), the scope of the incident, and the explainable effects on the data subject's situation. This approach helps to control the risk of "limitless harm" without reverting to national *de minimis* filters.[25]

In conclusion, once the threshold issue is addressed, the line should be drawn not by a barrier reduced to the question of "how serious?", but by a tripartite test: engagement of a protected rights-interest, case-specific substantiation, and concretisation of risk. This triad remains consistent with the broad compensatory aim of Recital 146, while preserving the infringement–damage distinction under Article 82 and preventing the regime from sliding into a practice of automatic compensation.

III. Evidentiary Challenges and Information Asymmetry in the Digital Environment

1. Structural Asymmetry in Proving Digital Harm: Who Holds the Information?

Because the GDPR contains no explicit rules on the burden of proof under Article 82, the evidentiary architecture of compensation claims is, in principle, governed by national procedural autonomy. That autonomy, however, is not absolute. Claims derived from EU law may not be subjected to less favourable conditions than comparable domestic claims principle of equivalence, and the exercise of such claims must not be rendered practically impossible or excessively difficult principle of effectiveness.[26]

This framework is of particular significance for digital infringements. Key facts such as the scope of the incident, the categories of data affected, the direction of data flows, the extent of access and dissemination, the duration of the security incident, and system logs typically lie within the controller's technical and organisational sphere of control.[27] In these circumstances, placing the entire burden of proving the infringement, the damage, and causation strictly on the claimant may render the right to compensation practically impossible to exercise.

---

[22] Lea Stegemann, *Der immaterielle Schadensersatz bei Datenschutzverstößen* (Nomos 2024) s. 260.
[23] Mulders (n 18), s. 1.
[24] ibid 5. s. 8-10.
[25] Stegemann, L. (n 22), s. 255
[26]Quaas in Heinrich Amadeus Wolff, Stefan Brink and Antje von Ungern-Sternberg (eds), BeckOK Datenschutzrecht (52nd edn, C H Beck, updated 1 May 2025) DS-GVO art 82 para 51.
[27] OLG Stuttgart (4. Zivilsenat), Urteil vom 26 June 2024 – 4 U 172/23, GRUR-RS 2024, 15776, para 36.

This structural asymmetry is even more pronounced in claims for non-material damage. The claimant is expected not merely to allege that an infringement occurred, but also to concretise the adverse effect experienced and to establish a legally relevant causal link between the infringement and that effect. Yet such concretisation will often require access to information about the technical context of the incident. As a result, in the digital environment, evidentiary difficulty is no longer simply a matter of pleading; it becomes a structural problem rooted in factual control over information.
In digital disputes, the difficulty of proof thus stems less from the claimant's capacity to articulate a subjective narrative than from the fact that the technical information at the core of the dispute largely lies within the defendant's sphere of control.

2. Reconstructing the Evidentiary Architecture: Accountability (Article 5(2)) and the Secondary Burden of Substantiation

The accountability principle introduced by the GDPR has reshaped the traditional understanding of the burden of proof. Under this principle, controllers and processors are not only required to process personal data lawfully; they must also be able to demonstrate compliance through appropriate documentation. Accordingly, when assessing compliance particularly with the core principles set out in Article 5(1) GDPR (lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality) the practical centre of gravity of explanation and evidentiary documentation will, in many cases, lie with the controller.[28]
This does not amount to an unlimited obligation. Controllers are required to provide explanations only in relation to processes that fall within their own sphere of knowledge and control, are reasonably accessible, and are capable of being documented.[29] This approach is also consistent with the principle of proximity to evidence developed in the CJEU's competition-law case law: the party with superior access to the relevant evidence typically the controller should bear a corresponding duty to provide explanations and supporting documents, thereby mitigating the imbalance created by structural information asymmetries.[30] The GDPR's accountability principle does not eliminate the data subject's burden of proof; however, the controller's duty to provide detailed explanations and documentation serves to counterbalance information asymmetries.[31]
German case law also confirms this approach. In a decision of the Regional Court of Oldenburg , the court held that, as a rule, the claimant bears the burden of proving the GDPR's temporal applicability. However, where the claimant lacks access to the relevant facts, the defendant must under the secondary burden of substantiation carry out reasonable inquiries and respond to the allegations with sufficient specificity.[32] In a decision of the Higher Regional Court of Stuttgart , the court held again in a scraping context that, as a rule, the claimant bears the burden of proving the GDPR's temporal applicability. However, because the claimant cannot be expected to know the internal facts of the incident and the information relevant to the timing of the infringement lies within the defendant's sphere of control, the defendant was subject to a secondary burden of substantiation in relation to the date on which the infringement occurred.[33]

---

[28] Bergt (n 12) para 46.
[29] Quaas (n 26) para 53.
[30]Tim Wybitul, David Haß and Jan Philipp Albrecht, 'Abwehr von Schadensersatzansprüchen nach der Datenschutz-Grundverordnung' (2018) *NJW* 113, 115–18.
[31] *LG Landshut, GRUR-RS 2025, 1283, para. 22.*
[32] LG Oldenburg, GRUR-RS 2025, 1282, para 12.
[33] OLG Stuttgart (n 27) para 36.

The limits of the secondary burden of substantiation are as important as its function. The mechanism must not turn into a fishing expedition based on vague and open-ended information requests; rather, the duty to provide explanations should be confined to specific, proportionate factual matters that are relevant to resolving the dispute. Moreover, where disclosure would conflict with trade secrets, security sensitivities, or the rights of third parties, both the scope and the modalities of disclosure must be carefully balanced. Most importantly, this mechanism must not be operated as if it created a presumption of damage or causation; it should not erode the constituent elements of Article 82 or lead, in effect, to an automated compensation regime.

3. Causation and the Concretisation of Damage: From Abstract Inconvenience to Compensable Harm

Before the GDPR, significant divergences existed among Member States. For example, while a de minimis rule was not generally recognised in France and Belgium, jurisdictions such as Germany and the Netherlands typically awarded non-material damages only in cases involving a serious interference with personality rights. This diversity underscored the need for a more coherent approach after the GDPR entered into force. Accordingly, the GDPR shifted to the European level the debate over whether a high threshold should be required between a mere infringement and proof of non-material damage.

Under Article 82 GDPR, the claimant must demonstrate both that damage occurred and that this damage is linked to the data protection infringement. Proof of non-material damage is inherently difficult. In Österreichische Post [34] and Scalable Capital [35], the Court of Justice emphasised that the mere existence of an infringement does not, by itself, give rise to compensation; the claimant must show an individualised, concrete adverse effect. Likewise, in juris GmbH, the Court stated that the claimant must prove both the damage and the causal link; otherwise, the compensation claim must be dismissed. [36]

In this framework, courts expect claimants to substantiate, at an individual level, a concrete adverse effect and to justify the link between that effect and the infringement; mere statements of unease, anxiety, or discomfort are often not considered sufficient. At the same time, there is no uniform EU-level concept of causation, and the Court has not, to date, developed a fully articulated doctrine in this regard. Similarly, rules on evidence are procedural in nature and, as a matter of principle, fall within the domain of Member State law. [37].

This cumulative structure, while rejecting the idea of "automatic compensation for every infringement," also entails the risk that the requirement of concretisation will, in practice, be applied in a manner that reintroduces a seriousness threshold through the back door. A critical assessment should therefore show that, if courts set the "concrete adverse effect" threshold excessively high without taking account of the factual characteristics of digital infringements such as structural information asymmetries and the concentration of technical contextual information within the defendant's sphere of control Article 82 may become practically ineffective.

A similar screening logic operates in fear-of-misuse narratives. According to the CJEU line of reasoning reflected in the BGH's request for a preliminary ruling in VI ZR 258/24, fear that personal data may be misused in the future can, in principle, fall within the scope of non-material damage. However, that fear must be substantiated in light of the concrete circumstances of the case. The courts have stressed that a mere assertion of fear, without

[34] UI v Österreichische Post (n 2) para 42.
[35] Scalable Capital (n 17) para 42.
[36] Case C-741/21 *GP v juris GmbH* EU:C:2024:288, para 35.
[37] Mulders (n 18), s. 5.

demonstrated adverse consequences, is not sufficient, and that a purely hypothetical risk does not give rise to compensation.[38]

This approach requires that fear be linked not to an abstract possibility inherent in any infringement, but to an objective risk arising from the context of the concrete breach. At the same time, the technical facts needed to objectify that risk such as the categories of data involved, the scope of dissemination or access, the duration of the incident, and log data will often lie within the controller's sphere of control. For this reason, where courts raise the requirement of concretisation, they must also operate procedural counterbalances effectively most notably the accountability principle and the secondary burden of substantiation so as to ensure that the contextual information necessary to substantiate risk is brought before the court. Otherwise, the concretisation standard risks turning into a screening mechanism that, contrary to digital realities, makes the right to compensation excessively difficult to exercise.[39]

With respect to causation, the but-for test asking whether the harm would have occurred in the absence of the infringement and the notion of contributory causation, under which causation is not severed even where multiple contributing factors exist, are instructive for assessing multi-causal narratives of digital harm.[40] As indicated in Scalable Capital, even in scenarios involving a high level of risk, demonstrating "actual harm" and, in particular, establishing the source/attribution link may become practically excessively difficult where the identity of the wrongdoer and the data flows are unknown.[41] This reality sharpens the critique: if courts treat the concretisation of damage and causation as a screening mechanism without taking due account of attribution problems and structural information asymmetries, the practical operation of Article 82 may be narrowed to an extent that is no longer compatible with the EU-law principle of effectiveness.[42]

In conclusion, the key challenge for this section is to construct a balanced evidentiary architecture that preserves the CJEU's insistence that there is no automatic entitlement to compensation, while preventing the standard of concretisation in digital disputes from being raised to a level that would erode the principle of effectiveness. Put differently, Article 82 must neither be reduced to a regime of "automatic compensation" based solely on the infringement, nor be applied in a way that due to evidentiary asymmetries and tracing difficulties produces a de facto shield/immunity effect in favour of controllers. Striking this balance also provides the necessary foundation for the next step of the analysis, namely the assessment of how compensation should be quantified.

IV. Determining Compensation and Symbolic Forms of Redress

1. Quantification of Compensation: The Compensatory Principle and the Search for Objective Criteria

The question of how to quantify compensation under Article 82 GDPR has been clarified in the CJEU's case law, in particular through Krankenversicherung Nordrhein[43],

---

[38] BGH, Beschl. V. 28.08.2025 – VI ZR 258/24, Özellikle Rn. 49–50 ; ABAD, C-655/23, Case C-655/23 IP v Quirin Privatbank AG (CJEU, 4 September 2025) EU:C:2025:655, para 57–58.

[39] *BL v MediaMarktSaturn* (n 19) para 66–68; Case C-590/22 *AT and BT v PS GbR and Others* (CJEU, 20 June 2024) EU:C:2024:536, para 35.; *IP v Quirin Privatbank* (n 38) para 62.; LG Oldenburg, Urteil vom 17 January 2025 – 5 O 3325/23 (juris).; OLG Stuttgart, Urteil vom 26 June 2024 – 4 U 172/23 (juris).

[40] Aliprandi (n 9), s. 357 Ff.; Bergt (n 12), para 45.; Joachim Kohn, 'Der Schadensersatzanspruch nach Art 82 DS-GVO' (2019) ZD 498.

[41] Mulders (n 18), s, 5.

[42] Quaas (n 26) para 51.; Case C-403/16 *El Hassani* (CJEU, 13 December 2017) EU:C:2017:960, para 26; Case C-817/19 *Ligue des droits humains* (CJEU, 21 June 2022) EU:C:2022:491, para 297.

[43] Case C-667/21 *ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein* EU:C:2023:1022, paras 83 and 101.

MediaMarktSaturn [44], and juris GmbH. [45] In these judgments, the Court has underscored that the primary purpose of Article 82 GDPR is not punishment, but compensation for the damage suffered. In assessing the function of the provision, the Court has made clear that Article 82 is designed, first and foremost, to restore the injured person so far as possible to the position they would have been in absent the infringement, and therefore does not operate as an additional sanctioning mechanism with a punitive or deterrent character.

Against this background, the Court has stated that the criteria laid down in Article 83 GDPR for determining administrative fines such as the gravity and duration of the infringement, whether it is repeated, the controller's level of cooperation, or the degree of fault cannot be applied directly or by analogy when calculating compensation. Those factors are tailored to ensuring that administrative penalties are imposed in a proportionate and dissuasive manner, and they do not align with the function of damages as an instrument of individual redress. Accordingly, elements such as the seriousness or duration of the infringement, or the controller's degree of fault, cannot be treated as independent criteria that serve to increase the amount of compensation beyond what is necessary to make good the harm suffered. This approach reinforces the compensatory nature of Article 82 and confirms its non-punitive character, thereby drawing a clear functional distinction between compensation and administrative sanctions.

Relying on the principle of full and effective compensation (Recital 146), the CJEU holds that the amount awarded must fully cover the claimant's concrete harm. Compensation should, therefore, place the victim as far as possible in the pre-infringement position, but it must not contain any punitive or deterrent surplus. On that basis, the only benchmark for determining the amount is the material or non-material damage actually suffered by the victim. Moreover, the occurrence of multiple infringements affecting the same individual is not accepted as an independent factor justifying an increased award. Rather, the amount payable must compensate the victim's overall harm, but should not be raised by taking into account the number of infringements or their repetitive character.

The judgment in Quirin Privatbank further concretises the compensatory principle for the purpose of quantification. While a "loss of control" in the context of an infringement and fear of future misuse may, under certain conditions, be assessed as non-material damage, the amount of compensation must be based not on abstract assumptions but on whether under the concrete circumstances of the case the fear/effect is sufficiently substantiated and on its intensity. A mere assertion or an entirely hypothetical risk, taken alone, should not be regarded as sufficient for compensation (and therefore for the quantum).[46]

At the same time, the CJEU has emphasised that Article 82 does not lay down any concrete criteria and that, accordingly, the determination of the amount of compensation is left to the national laws of the Member States. That discretion, however, is constrained by the EU-law principles of equivalence and effectiveness. In other words, compensation for data protection infringements under national law must not be treated less favourably than comparable claims, and it must secure the effective protection of victims' rights.[47]

These decisions do not set out explicit or systematic criteria for determining the amount of compensation. They do, however, indicate that courts tend to base quantification primarily on the nature of the data and the concrete effects of the infringement on the victim.

The BGH's referral in VI ZR 258/24 further highlights the practical significance of the limits of compensation. It points to scenarios in which an infringement is deliberately provoked and damages claims become a revenue model, illustrating how the compensatory function of

[44] *BL v MediaMarktSaturn* (n 19), para 53.
[45] *GP v juris GmbH* (n 36) para 57.
[46] *IP v Quirin Privatbank* (n 38).
[47] *GP v juris GmbH* (n 36) para 58ff.

Article 82 may be eroded with relative ease. Although the referral does not itself codify criteria for quantification, it is important in that it shows how the risk of damages turning into a punitive instrument responding to the infringement as such rather than compensating harm directly affects the regime's legitimacy and coherence.[48]

In conclusion, while the CJEU's case law correctly draws the line between "punishment" and "compensation", national proceedings continue to face a risk that this framework will oscillate between two extremes: on the one hand, an approach that effectively turns damages into a quasi-sanctioning uplift, and on the other, practical ineffectiveness due to difficulties of concretisation and attribution—often reflected in very low or merely symbolic awards that risk hollowing out the promise of "full and effective compensation" (Recital 146). Accordingly, the debate extends beyond how to determine the amount of compensation to the question under which limits non-monetary forms of redress (such as an apology) may be considered within the system of Article 82 GDPR.

2. Possibility of Non-Monetary Redress for Non-Material Damage: Apology and the Limits of the "Full Compensation" Requirement (C-507/23 PTAC)

Article 82 GDPR is primarily concerned with monetary compensation for material and non-material damage. Recent case law of the Court of Justice, howevermost notably C-507/23 (PTAC) has brought to the fore the question whether "alternative" or "complementary" forms of redress may be available. In the case at hand, the referring court asked whether an apology, on its own, could amount to sufficient redress, or whether monetary payment is necessarily required.

First, the Court reaffirmed its established line of authority: a mere infringement of the GDPR does not, as such, give rise to liability in damages. To obtain compensation, the claimant must demonstrate actual damage and a causal link between the infringement and that damage. It follows that not every infringement automatically translates into compensation under Article 82; the victim must show that the infringement produced harm in their particular case.

Second, the Court addressed whether an apology either alone or in addition to monetary compensation can qualify as an appropriate form of redress. While accepting in principle that an apology may constitute a means of redress, the Court stressed that this is possible only if the apology is capable of fully remedying the harm. The criteria by which this assessment is to be carried out are left to the discretion of national courts; the Court focuses less on the form and sincerity of the apology than on the outcome namely, whether, in the circumstances of the case, the harm has actually been remedied.

In this respect, the C-655/23 line of case law indicates that the approach taken in PTAC must be read together with the compensatory logic of Article 82: the Court emphasises that an apology (or comparable non-monetary forms of redress), provided that it is recognised under national law, may be taken into account only insofar as it produces a compensatory effect in the circumstances of the case. Accordingly, particularly where the harm has concrete and lasting repercussions, whether an apology alone can ensure "full compensation" remains a matter that national courts must examine separately.[49]

Third, responding to a question referred by a Latvian court, the Court examined whether the controller's intent or good faith conduct can justify a reduction in the amount of compensation. The Court rejected this possibility, stressing that Article 82 is concerned solely with compensating the damage suffered and does not incorporate punitive or "discounting" criteria. Accordingly, the controller's good faith, or the fact that processing pursued a public interest aim, cannot lead to the victim's harm being valued lower. At the same time, this raises a further

[48] BGH, Beschluss vom 28 August 2025 – VI ZR 258/24, ECLI:DE:BGH:2025:280825BVIZR258.24.0.

[49] *IP v Quirin Privatbank* (n 38), para 79.

question: if apologies are accepted as a form of redress, how should courts ensure that an apology is not treated merely as evidence of the wrongdoer's "good faith," rather than being assessed strictly by reference to whether it fully remedies the harm?[50]

In C-655/23, the Court emphasises that compensation under Article 82 (particularly in relation to non-material harm) serves an "exclusively compensatory" function and therefore that factors such as the gravity of the infringement or the controller's intent and motives cannot be used to reduce the amount of compensation or otherwise weaken the form of redress to the detriment of the victim; against this background, an apology should not operate as a good-faith discount, but may be considered as an independent form of redress only where it is provided for under national law and is capable, in the circumstances of the case, of ensuring full compensation. The same judgment further clarifies that an injunction/prohibitory order preventing repetition is purely preventive in nature and thus cannot be taken into account to reduce monetary compensation under Article 82 or to replace it in whole or in part, confirming that not every non-monetary measure has the same status within the Article 82 framework and that only measures capable of producing a compensatory effect (such as an apology) can, in principle, be discussed in this context. [51]

In conclusion, the CJEU's approach does not treat an apology as a definitive solution, but rather frames it as a cautious possibility that must be assessed in the specific case against the standard of full compensation. In this framework, the adequacy of an apology will be reviewed by national courts not primarily in terms of the victim's subjective satisfaction, but by reference to whether "full compensation" has been achieved in legal terms thereby highlighting the need for more reviewable and workable criteria in practice.

IV. Conclusion and Future Outlook

Article 82 GDPR is a multi-layered and dynamic provision designed to safeguard individuals' control over their personal data in the digital age and to hold controllers to account. The analysis developed in this article suggests that the compensatory function of Article 82 can be realised only if non-material damage is applied as an autonomous concept of EU law, freed from the restrictive filters of national legal orders. The Court of Justice's case law—most prominently in Österreichische Post and along the PTAC line—has rejected artificial barriers such as a minimum seriousness threshold (a de minimis approach), thereby expanding individuals' effective access to judicial redress. This expansion raises further questions: how to draw a qualitative boundary between "damage" and mere inconvenience, and how to concretise proof under conditions of digital (informational) asymmetry. In this respect, the secondary burden of substantiation and the accountability principle are indispensable tools for reconstructing the evidentiary architecture and mitigating information asymmetries.

With respect to non-pecuniary remedies, the apology debate in the PTAC line of case law adds a further layer of uncertainty. Since an apology can be contemplated only in principle and is constrained by the requirement of full compensation, the central issue is not whether an apology is available, but under what conditions it can be regarded as genuinely compensatory. How national courts will assess factors such as the apology's scope, addressee, degree of publicity, and its practical capacity to remedy the harm will shape the trajectory of this strand of litigation. In this context, a delicate balance emerges between concerns that apologies may become a low-cost substitute for monetary redress and critiques that, for certain harms, monetary compensation risks becoming merely symbolic.

Looking ahead, three trends under Article 82 GDPR appear particularly worth monitoring. First, as the Court's insistence that there is no automatic entitlement to compensation becomes

[50] Case C-507/23 A v Patērētāju tiesību aizsardzības centrs (CJEU, 4 October 2024) EU:C:2024:854.; Ruben Schneider, 'Anm zu EuGH, Urt vom 4 October 2024 – C-507/23' (2025) ZD 22.

[51] *IP v Quirin Privatbank* (n 38) para 70–72, 80–83.

more pronounced, the debate over where to set the standard of concretisation will gain further salience. Second, as data breaches increasingly take on an ecosystem character through practices such as scraping, intermediary data markets, and chain transfers, questions of attribution and causation are likely to arise more frequently. This may prompt courts to develop refined solutions regarding access to contextual information and the allocation of duties to explain. Third, the growing deployment of AI-based systems may render data flows more opaque and sharpen the question of who holds which information, generating demand for more methodical approaches both to proof and to the concretisation of risk.

Against this backdrop, the practical force of Article 82 hinges less on an abstract debate about "thresholds" than on the method by which courts construct the damage–risk–causation nexus. While the CJEU's framework pushes back against restrictive national filters, it leaves national courts with a twofold task: on the one hand, to stabilise an event-specific standard of concretisation without reinforcing perceptions of automatic compensation; on the other hand, to ensure that structurally entrenched information asymmetries in the digital ecosystem do not make proof practically impossible by counterbalancing them through the secondary burden of substantiation and the accountability principle. Non-pecuniary forms of redress, particularly apologies, will preserve their compensatory value only if their criteria are clarified and applied consistently with the logic of full compensation; otherwise, they risk becoming a low-cost substitute. Ultimately, the future of Article 82 depends on a balanced judicial architecture that safeguards the compensatory principle while enhancing predictability across explanatory duties, concretisation standards, and forms of redress.