UNIO - *EU Law Journal*. Vol. 11, No. 1, June 2025, pp. 146-155.
®2025 Centre of Studies in European Union Law
School of Law – University of Minho

Privacy *vs.* business convenience: the *Mousse* judgment and the future of data protection in the EU

João Pedro Sousa[*]

ABSTRACT: The Mousse *ruling represents a pivotal moment in EU data protection law, reinforcing strict limitations on personal data processing and clarifying the legal standards under the General Data Protection Regulation (GDPR). The Court of Justice of the European Union (CJEU) reaffirmed that data collection must be objectively indispensable for a specified legal basis, rejecting broad interpretations of contractual necessity and legitimate interest. Additionally, the ruling confirms that the right to object cannot retroactively justify unlawful data processing, thereby strengthening consumer rights and tightening compliance obligations for businesses. By aligning with important EU legislative initiatives, the ruling sets a robust precedent for future interpretations of data protection law, influencing regulatory enforcement, corporate practices, and the evolving digital economy. Additionally, the judgment highlights the broader role of personal data protection as a safeguard for digital citizenship, reinforcing the strict application of Article 8 CFREU in the face of increasing corporate data practices.This paper will analyse the* Mousse *ruling in detail, beginning with an overview of the facts of the case, followed by a discussion of the relevant legal framework and the findings of the Court. The analysis will then explore the ruling's implications for EU law and policy, particularly in balancing fundamental rights with economic interests. The study concludes with a critical assessment of the ruling's potential impact on future EU data protection jurisprudence and the broader digital economy.*

KEYWORDS: GDPR – principle of necessity – principle of proportionality – contractual necessity – consumer rights.

[*] Master's Student in European Union Law at the School of Law of the University of Minho.

1. Introduction

Data protection has become one of the defining legal issues of the digital age, with the European Union (EU) at the forefront of developing a regulatory framework that safeguards individual rights while ensuring businesses can operate efficiently.[1] The General Data Protection Regulation (GDPR)[2] enshrines principles such as data minimisation and lawfulness of processing, restricting personal data collection and its use to what is strictly necessary.[3] However, as technology advances[4] and commercial practices evolve, tensions often arise between privacy rights and business convenience. The Court of Justice of the European Union (CJEU) frequently intervenes to clarify these legal grey areas, as it did in the *Mousse* case.[5]

Firmly rooted in primary and secondary EU legislation, data protection is established under the Treaty on the Functioning of the European Union (TFEU),[6] the Charter of Fundamental Rights of the European Union (CFREU),[7] and the GDPR. The CJEU has consistently reaffirmed that while data protection is a fundamental right, it is not absolute and must be balanced against other fundamental rights and legitimate interests in line with the principle of proportionality.[8] This balance was central to *Mousse*, a case that questioned the extent to which businesses can impose mandatory data collection practices in the name of commercial convenience.[9] However, beyond its immediate implications for data processing under the GDPR, the case also underscores the broader importance of personal data protection as a pillar of digital citizenship.[10]

This paper examines the recent *Mousse* judgment (case C-394/23), a significant ruling that clarifies the scope of the GDPR's principles of data minimisation and lawfulness of processing in the context of online commercial transactions.[11] The case originated from a dispute between *Mousse*, a French association advocating for LGBTIQ+ rights, and the *Commission Nationale de l'Informatique et des Libertés* (CNIL), concerning the legality of SNCF Connect's requirement for customers to disclose their title (either "Monsieur" or "Madame") when purchasing travel documents online.[12]

---

[1] Alessandra Silveira, "Princípio do respeito aos direitos fundamentais", in *Princípios de direito da União Europeia* (Lisboa: Quid juris, 2011), 79-102.

[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, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, May 4, 2016, 1–88.

[3] Specifically Articles 5(1)(c) and 6(1) of the GDPR.

[4] Alessandra Silveira, "Pensar sem corrimão: sobre a regulamentação de tecnologias disruptivas e a proteção de direitos fundamentais na União Europeia", in *As palavras necessárias - Estudos em comemoração dos 30 anos*, 14 December 2023 (Braga: Universidade do Minho, 2024), https://doi.org/10.21814/uminho.ed.148.1.

[5] Judgment *Mousse v. CNIL and SNCF Connect*, 9 January 2025, case C-394/23, ECLI:EU:C:2025:2.

[6] Article 16 TFEU.

[7] Tiago Sérgio Cabral and Alessandra Silveira, "Commentary to Article 8" in *The Charter of Fundamental Rights of the European Union: A Commentary*, ed. Alessandra Silveira, Larissa Araújo, Maria Inês Costa and Tiago Sérgio Cabral (Braga: UMINHO Law School / JusGov, 2024), 100.

[8] *Mousse*, para. 24.

[9] *Mousse*, para. 18.

[10] European Parliament and the Council of the European Union, European Declaration on Digital Rights and Principles for the Digital Decade, 2023/C 23/01, PUB/2023/89, OJ C 23, 23 January 2023, 1–7.

[11] *Mousse*, para. 1.

[12] *Mousse*, para. 13.

This case raises a fundamental question: to what extent can private enterprises impose mandatory data collection practices for commercial convenience, and how does this align with the EU's commitment to protecting personal data? The ruling provides critical insights into the interpretation of Article 5(1)(c) GDPR (data minimisation), Article 6(1) GDPR (lawfulness of processing), and Article 21 GDPR (the right to object to processing).[13] Furthermore, the judgment raises broader implications regarding the intersection of data protection, non-discrimination, and freedom to conduct business under EU law.[14]

This paper will analyse the *Mousse* ruling in detail, beginning with an overview of the facts of the case, followed by a discussion of the relevant legal framework and the findings of the Court. The analysis will then explore the ruling's implications for EU law and policy, particularly in balancing fundamental rights with economic interests. The study concludes with a critical assessment of the ruling's potential impact on future EU data protection jurisprudence and the broader digital economy.

2. Facts of the case

The case of *Mousse v. CNIL and SNCF Connect* originated from a complaint filed by Association Mousse, a French advocacy organisation focusing on LGBTIQ+ rights, against the CNIL, France's data protection authority. The dispute concerned the data processing practices of SNCF Connect, the digital ticketing service of the French national railway company.[15]

SNCF Connect required customers to select a binary title ("Monsieur" or "Madame") when purchasing train tickets online. Mousse complained to the CNIL, arguing that this requirement violated the principle of data minimisation under Article 5(1)(c) GDPR, as the collection of this information was neither necessary for the provision of transport services nor justified under any lawful basis for processing under Article 6(1) GDPR.[16]

The CNIL dismissed the complaint, holding that the processing was lawful under Article 6(1)(b) GDPR, as it was necessary for the performance of a contract between SNCF Connect and its customers, ensuring personalised customer communication and providing a high standard of service. It further reasoned that addressing customers using their title aligned with common commercial practices and did not constitute excessive data collection.[17]

Dissatisfied by CNIL's assessment, Mousse challenged the decision before the *Conseil d'État*, the highest administrative court in France, which referred the case to the CJEU under Article 267 TFEU, seeking a preliminary ruling on the compatibility of SNCF Connect's practice with EU law. The referral posed two key questions: *i)* Whether the collection of customers' titles for commercial communication complies with data minimisation under Article 5(1)(c) GDPR and *ii)* whether it qualifies as necessary processing under Article 6(1)(b) and (f) GDPR.[18]

Whether, in assessing the necessity of the compulsory collection and processing of customer titles – even when some customers do not identify with either of the two

[13] *Mousse*, paras. 4-10.
[14] *Mousse*, para. 64.
[15] *Mousse*, para. 13.
[16] *Mousse*, para. 14.
[17] *Mousse*, para. 15.
[18] *Mousse*, para. 19.

options and consider the collection irrelevant – account should be taken of the fact that these customers may later exercise their right to object to the use and storage of their data under Article 21 GDPR.[19]

By addressing these questions, the CJEU was tasked with clarifying the limits of data collection in commercial transactions and balancing privacy rights against business practices.

3. Legal context and framework

The *Mousse* case is embedded in the broader framework of EU data protection law, primarily governed by the GDPR, the CFREU, and the TFEU. At its core, the case concerns the lawfulness of personal data processing under Article 6(1) GDPR, the principle of data minimisation under Article 5(1)(c) GDPR, and the extent to which a right to object under Article 21 GDPR affects the legality of data collection. The Court was asked to clarify whether the mandatory collection of customers' titles by SNCF Connect was justified under the GDPR and whether this requirement was objectively necessary and proportionate.

As a fundamental right, data protection is explicitly recognised in Article 8(1) CFREU and Article 16(1) TFEU, which guarantee that *"everyone has the right to the protection of personal data concerning them."* However, as the Court has consistently held, this right is not absolute and must be weighed against other fundamental rights and interests in accordance with the principle of proportionality.[20] This principle was central to the Court's analysis in *Mousse*, particularly in assessing whether SNCF Connect's data collection practice was necessary and proportionate considering the GDPR's provisions.

Under Article 5(1)(c) GDPR, the principle of data minimisation requires that personal data be adequate, relevant, and limited to what is necessary for the processing. Mousse argued that collecting customers' titles was unnecessary for the provision of transport services and, therefore, breached this principle.[21] In response, SNCF Connect and CNIL relied on Article 6(1) GDPR, which provides the legal basis for lawful data processing. Their primary argument was based on Article 6(1)(b) GDPR, which permits data processing where it is necessary for the performance of a contract.[22] They also invoked Article 6(1)(f) GDPR, which allows data processing when necessary for the legitimate interests of the controller, provided that such interests do not override the fundamental rights and freedoms of the data subject.[23]

The Court's assessment of these provisions required engagement with its prior case law on necessity and proportionality in data protection. In case C-252/21, *Meta Platforms and Others*, the Court held that contractual necessity under Article 6(1)(b) GDPR must be interpreted strictly, requiring that data processing be objectively indispensable for fulfilling a contractual obligation.[24] Applying this reasoning in *Mousse*, the Court determined that personalising commercial communication based on customers' titles was not objectively indispensable for the sale of train tickets.[25]

[19] *Mousse*, para. 19.
[20] *Mousse*, para. 24.
[21] *Mousse*, para. 16.
[22] *Mousse*, para. 32.
[23] *Mousse*, para. 44.
[24] Judgment *Meta Platforms and Others*, 4 July 2023, case C-252/21, ECLI:EU:C:2023:537, para. 92.
[25] *Mousse*, para. 39.

The principle of necessity was further reinforced by case C-439/19, *Latvijas Republikas Saeima (Penalty Points)*, where the Court ruled that data processing must be strictly necessary for the specific purpose it serves and that any less intrusive alternative must be considered.[26] The *Mousse* judgment applied this principle by examining whether SNCF Connect could have achieved its commercial objectives through alternative, less intrusive means.[27]

A separate legal issue in the case concerned Article 21 GDPR, which grants individuals the right to object to data processing based on legitimate interest. The *Conseil d'État* referred a question to the CJEU on whether the ability of customers to later object to the collection of their title was sufficient to justify the initial processing.[28] In line with its established case law, the Court ruled that the lawfulness of data processing must be assessed at the moment of collection and cannot be legitimised retroactively by the possibility of objection.[29]

Finally, the principle of proportionality played a decisive role in the Court's legal analysis. Under EU law, any restriction on fundamental rights must be necessary and proportionate to the objective pursued. In case C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, the Court ruled that derogations from data protection rights must be strictly necessary and proportionate.[30] The *Mousse* judgment applied this test by assessing whether SNCF Connect could have achieved its objective without collecting customers' titles.[31]

The legal context of *Mousse* thus required the Court to balance the right to personal data protection against commercial interests, while applying CJEU case law on necessity, proportionality, and lawfulness of processing. The Court's ruling clarified that the collection of customers' titles was not objectively necessary, thereby reinforcing the strict interpretation of necessity under the GDPR and further limiting the ability of businesses to justify non-essential data processing.

4. Findings of the Court

The CJEU ruled on whether SNCF Connect's mandatory collection of customers' titles was compatible with EU data protection law, particularly under the GDPR. It examined whether this requirement was necessary for contract performance under Article 6(1)(b) GDPR, justified as a legitimate interest under Article 6(1)(f) GDPR, and compliant with the principle of data minimisation in Article 5(1)(c) GDPR. The Court also considered whether the right to object under Article 21 GDPR could retroactively validate the processing.

Assessing contractual necessity, the Court reaffirmed that processing under Article 6(1)(b) GDPR must be objectively indispensable for fulfilling a contractual obligation.[32] It found that SNCF Connect's requirement for customers to select a title was not strictly necessary for ticket sales or transport services, as the contract

[26] Judgment *Latvijas Republikas Saeima (Penalty Points)*, 22 June 2021, case C-439/19, ECLI:EU:C:2020:1054, para. 110.
[27] Mousse, para. 40.
[28] *Ibid.*, para. 19.
[29] *Ibid.*, para. 67-70.
[30] Judgment *Koninklijke Nederlandse Lawn Tennisbond*, 4 October 2024, case C-621/22, ECLI:EU:C:2024:858, para. 37-41.
[31] Mousse, para. 40.
[32] *Ibid.*, para. 33.

could be performed without collecting this information. Personalising customer communication did not constitute an essential contractual requirement, and effective communication could occur without gender-based identifiers.[33] Since a less intrusive alternative existed, the Court ruled that Article 6(1)(b) GDPR could not justify the processing.[34]

The Court then considered legitimate interest under Article 6(1)(f) GDPR, which requires a balance between the controller's interest and the data subject's rights. While acknowledging that customer communication and personalisation may constitute a legitimate interest, the Court found that the necessity condition was not met, as SNCF Connect could have used neutral, non-gendered forms of address instead.[35] Furthermore, it noted that customers had not been adequately informed that their data was being processed on this basis, contrary to Article 13(1)(d) GDPR.[36] The absence of transparency further undermined the lawfulness of the processing, leading the Court to reject Article 6(1)(f) GDPR as a justification.[37]

The principle of data minimisation in Article 5(1)(c) GDPR requires that personal data be limited to what is strictly necessary. It held that SNCF Connect's mandatory title collection exceeded what was necessary, as it was neither indispensable for ticket purchases nor required for communication.[38] The Court emphasised that a less intrusive, non-gendered alternative was available, reinforcing that the requirement was excessive and unnecessary.[39]

SNCF Connect argued that the data processing at issue also served to adapt transport services for night trains, where certain carriages are reserved for passengers sharing the same gender identity, and to assist passengers with disabilities.[40] However, the Court rejected this justification, emphasising that such a purpose does not warrant the systematic and generalised processing of all customers' titles, including those traveling during daytime or not requiring special assistance. It found this disproportionate and contrary to the principle of data minimisation under Article 5(1)(c) GDPR, reaffirming that data collection must be strictly limited to what is necessary for a specific and legitimate purpose. The judgment reaffirmed that if gender-related data is required for specific service provisions, such as night train reservations or accessibility assistance, it should be collected only from customers who explicitly request such a service, rather than imposing a blanket requirement on all passengers.[41]

The Court also addressed the right to object under Article 21 GDPR, clarifying whether customers' ability to object to data processing retroactively justified its lawfulness. The *Conseil d'État* had sought guidance on whether this right could legitimise prior data collection. The Court ruled that lawfulness must be assessed at the moment of collection and cannot be validated retroactively by the possibility of objection.[42] It referenced case C-446/21, *Schrems*, which confirmed

[33] *Ibid.*, para. 39.
[34] *Ibid.*, para. 40 and 43.
[35] *Ibid.*, para. 48.
[36] *Ibid.*, para. 52.
[37] *Ibid.*, para. 63.
[38] *Ibid.*, para. 24.
[39] *Ibid.*, para. 40.
[40] *Ibid.*, para. 41.
[41] *Ibid.*, para. 42.
[42] *Ibid.*, paras. 67–70.

that data processing must be strictly necessary and proportionate from the outset, and an opt-out mechanism cannot legitimise unlawful processing.[43] Applying this principle, the Court concluded that customers' ability to object later did not make the initial collection lawful.[44]

In its final ruling, the CJEU reinforced strict limitations on data processing under Articles 5(1)(c), 6(1)(b), and 6(1)(f) GDPR. Additionally, the Advocate General's Opinion closely aligned with the final ruling, emphasising that controllers must justify data collection with clear legal bases and consider less intrusive alternatives, further solidifying GDPR's fundamental principles.[45] The Court held that collecting customers' titles for personalising commercial communication was not objectively indispensable or essential for contract performance, making Article 6(1)(b) GDPR inapplicable. The Court also ruled that Article 6(1)(f) GDPR could not justify the processing if customers were not informed at the time of collection, if the processing was not strictly necessary, or if fundamental rights, particularly the risk of gender-based discrimination, prevailed over the controller's interest. Additionally, it confirmed that the existence of a right to object under Article 21 GDPR does not retroactively validate unlawful data processing.

This judgment reinforced the strict necessity requirement under the GDPR, making clear that businesses cannot collect personal data unless it is objectively indispensable. It also reaffirmed that less intrusive alternatives must always be considered and that customers must be fully informed at the time of collection. By limiting the ability of businesses to justify non-essential data collection, the ruling strengthened EU data protection law and ensured greater protection of individuals' fundamental rights.

5. Implications for EU law

The *Mousse* ruling reinforces strict data protection standards across the EU and will have lasting consequences for business compliance, consumer rights, and regulatory enforcement. It establishes clear limits on data collection, requiring companies to ensure that any personal data they collect is strictly necessary for a specific, legitimate purpose.[46] This decision will particularly affect e-commerce, digital services, and transport industries, where customer profiling and data-driven personalisation are common business practices.[47] Companies that collect excessive data without proving its necessity risk enforcement actions, fines, and reputational damage under the GDPR. Additionally, the ruling strengthens the data protection by design and by default principle under Article 25 GDPR, pushing businesses to implement privacy-first models rather than justifying unnecessary data collection later.[48]

The judgment also narrows the interpretation of contractual necessity under Article 6(1)(b) GDPR, following the Court's earlier ruling in *Meta Platforms and Others* (case C-252/21). The Court made it clear that businesses cannot process

[43] Judgment *Maximilian Schrems*, 4 October 2024, case C-446/21, ECLI:EU:C:2024:834, para. 50.
[44] *Mousse*, para. 70.
[45] Advocate General's Opinion, *Mousse v. CNIL and SNCF Connect*, case C-394/23, ECLI:EU:C:2024:610.
[46] *Ibid.*, para. 33.
[47] European Commission, "Online platforms and e-commerce". Accessed January 25, 2025. https://digital-strategy.ec.europa.eu/en/policies/online-platforms-and-e-commerce.
[48] *Mousse*, para. 41-42.

data under the guise of contract performance unless it is truly indispensable.[49] This stricter approach will impact industries that rely on broad interpretations of contractual necessity, including transportation, finance, and online platforms. Companies in these sectors must now carefully review their contracts and privacy policies to ensure that they only collect data that is objectively required for service delivery.[50]

The ruling further enhances consumer protection by restricting businesses from compelling users to disclose personal data that is not strictly necessary. This approach aligns with broader EU regulatory initiatives aimed at addressing exploitative data collection practices, including the Digital Markets Act (DMA)[51] and the Digital Services Act (DSA),[52] which impose obligations on large online platforms to mitigate unfair commercial practices. Consequently, companies will be required to implement more transparent data governance policies and provide consumers with substantive control over the processing of their personal information.[53]

Another important aspect of the ruling is its impact on the legal basis of legitimate interests under Article 6(1)(f) GDPR. The Court ruled that business interests cannot automatically override fundamental rights, particularly in cases where data processing may lead to discrimination.[54] This decision introduces stricter compliance obligations for businesses that use automated decision-making, AI-driven profiling, and personalised marketing. The ruling is also in line with the EU's AI Act[55] and Data Act,[56] which introduce additional safeguards for automated data processing. Companies relying on AI-based decision-making will now need to prove that their legitimate interests do not infringe on individual rights, reinforcing the GDPR's strong emphasis on fairness and transparency.[57/58]

The Court also clarified the limits of the right to object under Article 21 GDPR, ruling that it cannot be used to justify unlawful data collection after the fact.[59] This is a major development for digital platforms and social media

[49] *Ibid.*, para. 28.
[50] *Meta Platforms and Others*, para. 98.
[51] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). OJ L 265, October 12, 2022, 1–66.
[52] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). OJ L 277, October 27, 2022, 1–102.
[53] European Commission, The Digital Services Act package. Accessed January 25, 2025. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.
[54] *Mousse*, para. 64.
[55] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). OJ L, 2024/1689, July 12, 2024. ELI: http://data.europa.eu/eli/reg/2024/1689/oj.
[56] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act). OJ L, 2023/2854, December 22, 2023. ELI: http://data.europa.eu/eli/reg/2023/2854/oj.
[57] European Commission, European approach to artificial intelligence. Accessed January 25, 2025. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.
[58] Tiago Sérgio Cabral, *AI Regulation in the European Union: democratic trends, current instruments and future initiatives* (Master Thesis: University of Minho, 2019), 131 and following. https://hdl.handle.net/1822/74323.
[59] *Mousse*, para. 70.

companies, many of which have historically relied on opt-out models rather than obtaining explicit user consent.[60] These businesses may now face increased regulatory scrutiny and higher penalties if they continue to operate in ways that contradict the Court's interpretation of lawfulness and necessity.[61]

From a broader policy perspective, the Mousse ruling aligns with ongoing EU legislative efforts, such as the proposed ePrivacy Regulation, which seeks to limit non-essential data tracking and strengthen user privacy protections.[62] By ruling that a retrospective right to object does not validate unlawful data collection, the Court has reinforced the EU's commitment to strong privacy protections and user control over personal data.[63]

The *Mousse* ruling reinforces the EU's strong stance on data protection, setting clear limits on when businesses can collect and process personal data. By reaffirming necessity and proportionality requirements, the Court has strengthened compliance obligations for businesses, enhanced regulatory oversight, and further entrenched the GDPR's position as the global benchmark for data protection.[64]

The *Mousse* ruling also has implications beyond data protection, particularly in anti-discrimination law and LGBTIQ+ rights. By rejecting the mandatory collection of binary gender titles, the Court has reinforced the principle that personal data processing must not reinforce systemic discrimination. Etienne Deshoulières, legal representative for the claimant, highlighted that this decision has immediate legal effects across all 27 EU Member States, setting a precedent for future legal challenges against gender-based classification in commercial and administrative practices.[65] This ruling aligns with EU anti-discrimination frameworks,[66] potentially influencing gender recognition policies and legislative reforms aimed at ensuring greater inclusivity in data processing across the EU.

Fundamentally, the ruling reaffirms that individual privacy rights must take precedence over business convenience, marking a significant advancement in the EU's data protection framework.[67]

6. Conclusion

The *Mousse* ruling marks a significant development in EU data protection law, reinforcing strict necessity and proportionality requirements under the GDPR. The Court's decision ensures that businesses cannot collect personal data unless it is objectively indispensable, rejecting broad interpretations of contractual necessity

[60] TechCrunch, "Elon Musk's X targeted with nine privacy complaints after grabbing EU users' data for training Grok", 11 August 2024. Accessed January 25, 2025. https://techcrunch.com/2024/08/11/elon-musks-x-targeted-with-eight-privacy-complaints-after-grabbing-eu-users-data-for-training-grok/.

[61] Data Protection Commission, "Irish Data Protection Commission fines LinkedIn Ireland €310 million", 24 October 2024. Accessed January 25, 2025. https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million.

[62] European Commission, "Why a reform of ePrivacy legislation?". Accessed January 25, 2025. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.

[63] *Mousse*, para. 70.

[64] *Ibid.*, para. 64-70.

[65] ICLG, "Top EU court rules against gender-based data collection", 10 January 2025. Accessed January 25, 2025. https://iclg.com/news/22128-top-eu-court-rules-against-gender-based-data-collection.

[66] Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services. OJ L 373, 21 December 2004, 37–43.

[67] *Mousse*, para. 70.

and legitimate interest. This stricter approach will require companies across various sectors to reassess their data processing practices, prioritising compliance over convenience.

The ruling also strengthens consumer rights and regulatory enforcement, particularly by confirming that opt-out mechanisms cannot retroactively justify unlawful data collection. It aligns with broader EU legislative efforts, such as the DMA, DSA, and the AI Act, reinforcing transparency and accountability in data-driven business models. Additionally, the Advocate General's Opinion closely aligned with the final ruling, emphasising that controllers must justify data collection with clear legal bases and consider less intrusive alternatives, further solidifying GDPR's fundamental principles.

Most importantly, *Mousse* reaffirms the EU's strong commitment to privacy and data protection, setting a high compliance standard for businesses. As technological advancements continue to reshape the digital economy, this ruling will guide future legal interpretations, regulatory enforcement, and policy debates, ensuring that privacy remains a cornerstone of EU law.

Article received on 5 February 2025 and accepted for publication on 26 February 2025.