Docnr4

From: 5.1.2.e <5.1.2.e @mensenrechten.nl>
Date: Friday, March 13, 2026, 11:15 AM
To: "'postbus@eerstekamer.nl'" <postbus@eerstekamer.nl>
"'mary.fiers@eerstekamer.nl'" <mary.fiers@eerstekamer.nl>
"'cees.vandesanden@eerstekamer.nl'" <cees.vandesanden@eerstekamer.nl>
Subject: RE: Inbreng College op mondeling overleg Omnibus Digitaal en Omnibus AI 17 maart a.s. inclusief statement ENNHRI en equinet

---

Attachments:
Equinet-and-ENNHRI-Joint-Statement-on-the-Digital-Omnibus-Regulation-Proposals-on-AI-and-on-Data.pdf

---

Geachte mevrouw Fiers en geachte heer Van de Sanden,

In navolging van onderstaande mail, stuur ik u ook nog het aangekondigde statement van het Europese netwerk van mensenrechtenorganisaties ENNHRI en het Europese netwerk van gelijke behandelingsinstellingen, Equinet over de digitale omnibussen.

Vriendelijke groet,

5.1.2.e
Senior Politiek Beleidsadviseur mensenrechten

College voor
de Rechten
van de Mens

5.1.2.e (mobiel)
030 888 38 88 (algemeen)
www.mensenrechten.nl

Van: Secretariaat <secretariaat@mensenrechten.nl>
Verzonden: vrijdag 13 maart 2026 10:41
Aan: 'postbus@eerstekamer.nl' <postbus@eerstekamer.nl>; 'mary.fiers@eerstekamer.nl' <mary.fiers@eerstekamer.nl>; 'cees.vandesanden@eerstekamer.nl' <cees.vandesanden@eerstekamer.nl>
CC: 5.1.2.e <5.1.2.e @mensenrechten.nl>
Onderwerp: Inbreng College op mondeling overleg Omnibus Digitaal en Omnibus AI 17 maart a.s.

Geachte mevrouw Fiers en geachte heer Van de Sanden,

De Eerste Kamer heeft een parlementair behandelvoorbehoud geplaatst bij de Omnibus AI en de Omnibus Digitaal. Op 17 maart vindt een mondeling overleg plaats tussen uw commissies en de staatssecretaris van EZK, Willemijn Aerts en de staatssecretaris van J&V, Claudia van Bruggen, over de Nederlandse onderhandelingspositie in deze processen. Ter voorbereiding op dit overleg, wil het College voor de Rechten van de Mens u nog een aantal punten meegeven op basis van de laatste stand van zaken rond de omnibussen. Ook wil het College u graag een gerelateerde brief sturen namens ons Europese netwerk van nationale mensenrechteninstituten, ENNHRI. Deze vindt u ook in bijlage.

Het College is graag bereid om een en ander nader toe te lichten. Mocht u naar aanleiding van deze brief vragen of opmerkingen hebben dan kunt u hiervoor contact opnemen met 5.1.2.e politiek beleidsadviseur, via 5.1.2.e @mensenrechten.nl of telefonisch via 5.1.2.e

Met vriendelijke groet,

5.1.2.e
Coördinator Secretariaat

College voor
de Rechten
van de Mens

5.1.2.e (direct)
030 888 38 88 (algemeen)
www.mensenrechten.nl
Volg ons op LinkedIn, Mastodon, Bluesky, Instagram en YouTube

Equinet-ENNHRI Statement on the Digital Omnibus Regulation Proposals on AI and on Data

1. Introduction

This joint statement on behalf of Equinet (the European Network of National Equality Bodies) and ENNHRI (the European Network of National Human Rights Institutions), represents the collective voices of independent public equality and fundamental rights authorities (NEBs and NHRIs) across Europe. We base our joint recommendations on the expertise and experience of over 60 independent national authorities, established by constitution or law to promote and protect fundamental rights and equality in over 40 European states.

The European Commission's (the Commission) new digital simplification initiative, consists of two separate but interlinked legislative proposals: the Digital Omnibus Regulation Proposal, which suggests amendments to a number of pieces of data legislation, including notably the EU's General Data Protection Regulation (GDPR), and the Digital Omnibus on AI Regulation Proposal, which amends the EU Artificial Intelligence Act. ENNHRI and Equinet take note of European Commission's efforts to address practical challenges in implementing the EU's digital acquis, but emphasise that administrative simplification must not come at the expense of fundamental rights protection.

We are concerned that the proposed amendments are proceeding without adequate impact assessments and public consultation, risking the erosion of fundamental rights protections. We recall the Commission's responsibility to ensure transparent, timely and meaningful public consultations on EU law and policymaking processes and to conduct impact assessments of EU legislation and policies, in consultation with relevant human rights actors, including NHRIs and NEBs. This helps ensure compliance of EU legislation with the Treaties (Article 2 TEU) and the Charter, and aligns with the Commission's own Better

Regulation Guidelines[1], which include stakeholder consultation as "an essential element of policy preparation and review" and which require impact assessments for initiatives expected to have significant economic or social impacts.

The two Digital Omnibus regulation proposals comprise a comprehensive package, covering areas from data legislation to cybersecurity and privacy rules, and therefore warrant careful impact assessment. Although the Commission justifies this absence of an impact assessment due to the "technical" nature of the proposed amendments, our following recommendations and reasoning show that many of the proposed changes could have serious impacts on the protection of fundamental rights, going beyond mere technical amendments.

We also recall that the AI Act only entered into force on 1 August 2024, and most obligations are not currently planned to apply until 2 August 2026. It is not possible to meaningfully assess the impact or application of an instrument when its transposition is still ongoing. Changes to the AI Act could undermine not only the ongoing transposition and implementation but also the ability of the instrument to create legal certainty for deployers, providers and rightsholders. Further, the AI Act, like other EU digital laws, relies on the GDPR as a foundation for protecting some fundamental rights in the digital sphere. As a result, the proposed GDPR amendments would have broader downstream effects, potentially weakening the AI Act's safeguards in ways that go beyond their immediate scope.

While the following is not included in our core recommendations, we wish to draw attention to the potentially problematic implications of the creation of a new category of the so-called Small Mid-Caps (SMCs) as well as for broadening the weakening of compliance obligations for Small and Medium-sized Enterprises (SMEs). SMEs and SMCs account for the overwhelming majority of companies in Europe, meaning that regulatory simplifications tied primarily to

[1] Both ENNHRI and EQUINET have recently submitted responses to the Commission call for evidence on the revision of the EU's Better Regulation Framework recommending that the Commission ensures that any revisions strengthen the quality and legitimacy of EU decision-making by ensuring transparent, inclusive and accountable processes.

company size rather than to the level of risk posed by AI systems could have systemic implications for rights protection. While we recognise the legitimate objectives of avoiding disproportionate administrative burdens for smaller actors and supporting innovation, safeguards should be calibrated to the risks posed by AI systems rather than to the size of the provider.

2. Overview: Key recommendations on the Digital Omnibus proposals amending the AI Act and GDPR

We urge the co-legislators to maintain equality and fundamental rights safeguards as they consider the proposed amendments under the Digital Omnibus proposals. Efforts to simplify the digital rules should reflect a fundamental rights-based approach. To achieve this, we recommend to:

1. Preserve AI System Registration Requirements under Article 49(2) of the AI Act.
2. Safeguard Powers of Article 77 Fundamental Rights Authorities under the AI Act.
3. Maintain High-Risk AI System Timeline in Article 113, Chapter III of the AI Act.
4. Preserve Strict Necessity and Fundamental Rights Safeguards in Article 10(5) AI Act When Introducing Article 4a on Processing Special Categories of Personal Data.
5. Prevent significant weakening of AI developers' and deployers' responsibility to ensure AI literacy for their staff.
6. Reject the weakening of the definition of personal data under Article 4(1) of the GDPR.
7. Preserve key information obligations under GDPR Article 13.
8. Reject proposed amendment to Article 22 GDPR on automated decision-making.

3. Background: Role of Equality Bodies and NHRIs on Digital Rights

NHRIs and NEBs play a key role in protecting fundamental rights and equality in the digital space, including as designated authorities under Article 77 of the AI Act. Through complaints handling, guidance, own initiative legal proceedings, raising awareness, and engagement with governments, they already contribute to AI oversight and accountability and are key actors in monitoring and

implementing EU and international human rights and non-discrimination law across a wide range of policy areas. NHRIs have a broad human rights mandate to monitor compliance with all fundamental rights while NEBs' are legally empowered to promote equality, combat discrimination, support victims, and monitor discrimination under EU law.

The EU Standards Directives[2] set harmonised, minimum legally binding standards for NEBs' mandate, independence, resources, powers, and accessibility, requiring Member States to take concrete measures to guarantee the independence of NEBs and ensure their effectiveness in combatting discrimination and promoting equality, including notably where new competences are ascribed to such bodies. NHRIs are unique as they are accredited with an internationally accepted quality label, based on their compliance with the UN Paris Principles, which include standards on independence, a broad mandate to promote and protect all human rights, freedom to address any rights issue, annual reporting on the national human rights situation, and cooperation with national and international actors, including civil society.

Since the conception of the AI Act, Equinet and ENNHRI have consistently called for strong and effective equality and fundamental rights safeguards, including Equinet's recommendations for the AI Act trilogues, ENNHRI's Common Position on the AI Act, and the Joint Equinet and ENNHRI Statement on the AI Act Trilogue.

Given their roles and expertise, NHRIs and NEBs are well-placed to advise on amendments to both the AI Act and the GDPR since these changes directly affect the protection of fundamental rights and non-discrimination. The

[2] Directive (EU) 2024/1500 of the European Parliament and of the Council of 14 May 2024 on standards for equality bodies in the field of equal treatment and equal opportunities between women and men in matters of employment and occupation, and amending Directives 2006/54/EC and 2010/41/EU; and Council Directive (EU) 2024/1499 of 7 May 2024 on standards for equality bodies in the field of equal treatment between persons irrespective of their racial or ethnic origin, equal treatment in matters of employment and occupation between persons irrespective of their religion or belief, disability, age or sexual orientation, equal treatment between women and men in matters of social security and in the access to and supply of goods and services, and amending Directives 2000/43/EC and 2004/113/EC.

recommendations in this statement are made without prejudice to the mandate of Data Protection Authorities (DPAs) and with reference to the EDPB-EDPS Joint Opinion on the Digital Omnibus on AI published in January 2026. Rather, NHRIs' and NEBs' expertise can complement that of DPAs by highlighting how weakening data safeguards can undermine equality, accountability, and access to remedies, particularly for groups at risk of discrimination.

4. Recommendations for effective fundamental rights protection under the Digital Omnibus on AI and Digital Omnibus on Data Proposals

1. Preserve AI System Registration Requirements under Article 49(2) of the AI Act

Article 1(14) of the the Digital Omnibus on AI proposes deleting Article 49(2) of the AI Act. This would remove the obligation to register AI systems that providers claim are exempt from high-risk classification under Article 6(3), significantly reducing transparency and accountability. While Article 6(3) allows certain Annex III systems to be treated as non–high-risk if they meet strict conditions, Article 6(4) currently requires providers to document this assessment, and Article 49(2) ensures this information is made visible through registration in the EU database for high-risk AI.

Without this crucial safeguard, it would be almost impossible for affected individuals, Article 77 fundamental rights authorities, and other stakeholders to verify whether exemptions are being lawfully applied. Similarly, oversight would become extremely difficult, particularly for actors who do not have the technical capacity or enforcement powers of market surveillance authorities (MSAs). Stricter registration obligations are already required in EU legislation for other industries, for example for medical devices[3] and electrical and electronic equipment[4]. Removing registration requirements under the AI Act would weaken transparency, hinder access to remedies, and increase the risk of

[3] Article 31, Regulation (EU) 2017/745 of the European Parliament and of the Council, 5 April 2017, on medical devices.
[4] Article 16, Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE) (recast).

misuse of the Article 6(3) exemption, while offering little genuine administrative relief given the relatively light documentation burden. It is not clear that removing the registration obligation would produce any meaningful cost-cutting impact, which the Commission presents as the main rationale for the amendment.

Maintaining mandatory registration of AI systems under Articles 6(4) and 49(2) of the AI Act is also essential to ensure the effective operation of fundamental rights impact assessments (FRIAs), under Article 27, and to safeguard access to redress for affected individuals. Registration anchors risk classification and deployment visibility, enabling relevant authorities to verify whether Article 27 obligations have been correctly triggered and fulfilled, and allowing individuals to identify responsible actors where fundamental rights are impacted. In this way, mandatory registration supports coherent oversight and enforcement under Chapter VII and helps ensure that the AI Act's risk-based framework delivers meaningful fundamental rights protection in practice.

We recommend rejecting the proposed deletion of Article 49(2) and maintaining the full text of Article 6(4). Preserving these provisions is essential to ensure public accountability and trust, enable effective enforcement of safety rules, safeguard meaningful access to remedies for rights-holders, and prevent the erosion of core transparency mechanisms within the AI Act.

2. Safeguard Powers of Article 77 Fundamental Rights Authorities under the AI Act

Proposed amendments to Article 77 of the AI Act risk weakening the ability of fundamental rights authorities to exercise effective and independent oversight. Article 77 was designed to grant designated national authorities responsible for protecting fundamental rights, including NHRIs, NEBs and DPAs, the powers needed to scrutinise AI systems and address risks to rights. Article 1(26) of the Digital Omnibus on AI would amend this framework by restricting how these authorities can access information by introducing conditional language that may limit access, as well as by introducing cooperation obligations that may affect their independence.

Currently, Article 77 authorities have the power to request information and access to documentation necessary to fulfil their mandates without specifying

limits on who they can request it from. Under the Digital Omnibus for AI, revised Article 77(1) and new Article 77(1a) would require Article 77 authorities to obtain information only through MSAs, creating risks of delays, information filtering, and dependency on MSA capacity and willingness to act, while also increasing the administrative burden on MSAs. This could undermine the independence and effectiveness of Article 77 authorities. For NEBs designated as Article 77 authorities, this amendment could even conflict with other EU legislation, notably Article 8 of the EU Standards for Equality Bodies Directive (EU) 2024/1499, which states that NEBs must be enabled to conduct fact-finding, including effective rights to access the information and documents needed to determine whether discrimination has occurred. Likewise, in order to comply with the UN Paris Principles, all NHRIs must have free access to inspect and examine any documents without prior written notice in order to fulfil their mandate (General Observations of the Sub-Committee on Accreditation, 1.2)

In addition, conditional language introduced in the new Article 77(1a) creates legal uncertainty about access to information, since it suggests that access is subject to various requirements. While some conditions are appropriate (necessity, proportionality), this phrasing creates uncertainty about what limitations may be imposed. Moreover, the new Article 77(1b) requirement for Article 77 authorities and MSAs to "cooperate closely and provide each other with mutual assistance", while positive in principle, must take into account the available resources, distinct mandates, and the requirement of independence of NHRIs and NEBs.

To ensure effective oversight, we recommend preserving the direct documentation and information access powers of Article 77 authorities, in line with the original purpose of Article 77. We also recommend that any amendments should include clear, concise language that does not limit access. Moreover, the new requirement on mutual cooperation obligation should not affect the independence of Article 77 authorities nor place additional responsibilities on them. This is essential to ensure robust, coherent, and credible fundamental rights oversight within the EU AI framework. We suggest that the language on mutual assistance between MSAs and Article 77 authorities could be better placed in a recital.

3. Maintain High-Risk AI System Timeline in Article 113, Chapter III of the AI Act

Chapter III, Section 2 of the AI Act establishes core obligations for high-risk AI systems (such as those used in hiring, credit decisions, or law enforcement), including risk management, data governance, transparency, human oversight, and robustness and cybersecurity. These were purposely designed to apply after a two-year transition period to allow providers to prepare while ensuring timely protection of fundamental rights and public safety. Article 1(31) of the Digital Omnibus on AI proposes amendments that would delay these protections until the Commission confirms support measures are available, or until backstop dates in December 2027 or August 2028. This would allow high-risk AI systems to operate for years without fundamental safety and rights protections, creating immediate risks of discrimination, system failures, cyberattacks, and inability to prevent harm.

The Commission states the proposed delay is due to implementation challenges, such as delays in designating national competent authorities and conformity assessment bodies, and a lack of harmonised standards for the AI Act's high-risk requirements, guidance, and compliance tools. However, AI Act legal obligations are not dependent on the existence of voluntary harmonised standards, particularly where guidance already exists or is forthcoming, and only create presumption of conformity. In addition, the Commission had the option of issuing common specifications in the absence of standards, as set out in Article 41(1)(a)(ii) of the AI Act but has proposed delaying protections instead. Further, while delays in institutional readiness may affect enforcement, they do not justify postponing substantive safeguards. Moreover, these delays risk creating legal uncertainty for business and disadvantage responsible businesses that have already taken steps to prepare for compliance.

We urge the co-legislators to prioritise the timely implementation of the AI Act, ensuring that its provisions are applied in practice as soon as possible, preferably by the original 2 August 2026 deadline, and, in any event, with minimal delays. Maintaining the original timeline would help reduce risks of discrimination, and other preventable fundamental rights harm, while supporting responsible innovation and public trust in AI systems.

4. Preserve Strict Necessity and Fundamental Rights Safeguards in Article 10(5) AI Act When Introducing Article 4a on Processing Special Categories of Personal Data

The proposed replacement of Article 10(5) AI Act with a new Article 4a under the Digital Omnibus on AI would significantly expand the legal basis for processing special categories of personal data, such as race, religion, sexual orientation, or political views, for bias detection and correction. It could extend this processing beyond high-risk AI systems to all AI systems and models, at both development and deployment stages.

While we generally endorse the suggested expansion of the legal foundation that permits the exceptional handling of such personal data, we emphasise that the processing of special categories of personal data for bias detection and correction could entail additional risks to the fundamental rights of affected persons. Given the evidenced tendency of AI systems to generate and propagate bias at a scale and speed which challenges the enforcement and supervision capacities of any public authority, the collection of sensitive personal data requires robust safeguards, clear justification and should be proportionate.

While Article 4a seems to be built on the idea that the risk of discrimination justifies the processing of special category data, a distinction should be drawn between (i) the legal and technical possibility to collect sensitive data *ex post* for supervision or auditing purposes, and (ii) the legal and technical necessity to collect such data *ex ante* for bias detection during system development. Both may be legitimate under robust safeguards, but they are conceptually different. If the derogation is justified by discrimination risks, proportionality would suggest that processing should be limited to what is demonstrably necessary and tied to concrete anti-discrimination obligations. Otherwise, the framework risks normalising sensitive data collection without ensuring that it meaningfully contributes to bias detection or correction. Further, we are concerned that the proposed amendment could effectively legitimise a substantial increase in the scale and scope of the collection of sensitive data to cover all AI systems and the main kinds of operators on the market.

If the proposed amendment is aimed at respecting rights, it requires the same safeguards as the current Article 10(5), namely the availability of appropriate technical and organisational measures, limitation to a specific purpose, the application of minimisation and proportionality principles, and compliance with the GDPR. However, the amendment introduces a potential weakening by including the vague qualifier 'as appropriate' in relation to the applicability of the *entire* list of safeguards in the amended text. The current formulation requires "appropriate safeguards," but in the absence of implementing guidelines specifying evaluation criteria for 'appropriateness', and without a framework for systematic institutional oversight of the scale necessary to detect biases in all AI systems, it would be difficult to verify and enforce these measures. The formulation risks creating divergent interpretations and possible abuses, opening the door to wider profiling and surveillance based on sensitive traits that are associated with heightened vulnerability and the need for stronger protections.

We recommend preserving the existing strict necessity criterion that governs the processing of special categories of personal data for bias detection and mitigation concerning high-risk AI systems under Article 10(5) of the AI Act.

5. Prevent significant weakening of AI developers' and deployers' responsibility to ensure AI literacy for their staff

The Digital Omnibus on AI proposes an amendment to Article 4 of the AI Act that would replace the current binding obligation on providers and deployers to ensure AI literacy among their staff with a non-binding duty on the European Commission and Member States to merely "encourage" such measures. This fundamentally shifts responsibility away from the private actors who develop and deploy AI systems and removes a clear, enforceable requirement that those directly developing and operating AI tools understand their functioning, risks, limitations and potential impact on fundamental rights.

Without mandatory AI literacy obligations, staff using systems in sensitive contexts such as recruitment, benefits administration or public services may be unable to assess fundamental rights risks and impacts, and to design and implement effective prevention and mitigation measures. Given that most AI development and much deployment occur in the private sector, replacing a

direct obligation with a significantly weaker promotional approach risks creating a significant enforcement gap. Moreover, this would effectively mean shifting responsibility to the often already under-resourced public sector.

We urge the co-legislators to maintain the binding AI literacy requirement in Article 4 to ensure that responsibility remains with those who design and use AI systems and to safeguard meaningful fundamental rights protection.

6. Reject the weakening of the definition of personal data under Article 4(1) of the GDPR

Proposed amendments in Article 3(1) of the Digital Omnibus would weaken the GDPR's definition of personal data by introducing a relative and subjective approach. Under this approach, information could be treated as non-personal if a specific entity cannot identify an individual, even where others could or where a future recipient may be able to do so, departing from the GDPR's objective standard of identifiability. This may allow entities to claim data is not personal based on their own capabilities, creating enforcement gaps, legal uncertainty, and incentives to engineer pseudonymisation loopholes. This risks fragmentation, weakens accountability, and departs from the CJEU's protective interpretation of identifiability. These changes could reduce accountability, weaken oversight, depart from other EU rules and caselaw, and make it harder for individuals to exercise their data protection rights.

We recommend that the co-legislators should preserve the GDPR's strong and well-established definition of personal data in Article 4(1) and Recital 26, which has proven essential for enabling consistent enforcement and ensuring robust protection of fundamental rights across the EU. Article 4(1) GDPR defines personal data as any information relating to an identified or identifiable person, including direct and indirect identifiers or unique characteristics. Recital 26 adds that identifiability depends on whether someone can be identified using means reasonably likely to be used. This scope aligns with Article 8 of the EU Charter

and established CJEU case law[5], and provides legal clarity for individuals, regulators, and organisations alike.

7. Preserve key information obligations under GDPR Article 13

Proposed amendments to GDPR Article 13 under Article 3(5) of the Digital Omnibus risk weakening the existing transparency framework by significantly expanding exemptions from obligations related to the collection of personal data. Currently, Article 13 requires controllers to give individuals key information when collecting their personal data, including the controller's identity, purpose and legal basis, legitimate interests pursued (if applicable), recipients, retention periods, rights, and whether automated decision-making is involved. This information must be provided " when personal data are obtained" (Article 13(1)). Article 13(4) currently exempts controllers from these obligations only where "the data subject already has the information."

The amendments expand exemptions based on vague language, such as the existence of a "clear and circumscribed relationship" or beliefs that individuals already know how their data is used (unless the data is shared, transferred internationally, used for automated decision-making, or poses high risk). This replaces a clear standard with a subjective assumption that people already know key information, making it harder to exercise their rights and potentially undermining transparency. Recently, the EDPB and the EDPS also called for maintaining "carefully limited and clearly defined conditions in Article 13(4) GDPR, also in light of the principle of proportionality, to ensure that the new exemption to the provision of information effectively leads to a reduction of the administrative burden for controllers" in a joint opinion.

A new Article 13(5) is also introduced which would allow researchers to rely solely on making information publicly available rather than contacting data subjects, without rules on where or how the information must be shared. While we support public research, it must not be conducted at the expense of leaving affected data subjects uninformed.

[5] See, inter alia, CJEU judgements *Meta v. Bundeskartellamt* (C-252/21), *Breyer* (C-582/14), *Nowak* (C-434/16), *YS and Others* (C-141/12 and C-372/12).

We call on the co-legislators to preserve and strengthen the transparency framework under GDPR Article 13. Maintaining the current clear standard provides legal certainty for controllers while ensuring trust, accountability, and the effective exercise of data protection rights for individuals.

8. Reject proposed amendment to Article 22 GDPR on automated decision-making

The proposed amendment to Article 22 GDPR under Article 3(7) of the Digital Omnibus would significantly alter the structure of protection against fully automated decision-making that produces legal or similarly significant effects. As interpreted by the Court of Justice of the European Union, Article 22(1) establishes a prohibition in principle, subject only to limited exceptions[6]. The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have likewise emphasised in their recent opinion on the Digital Omnibus that the provision must be framed as a prohibition with narrowly defined derogations and cautioned against wording that could be read as transforming it into a broad authorisation regime that might create the impression that automated decision-making is, as a rule, permissible whenever it is related to entering into, or performing a contract (e.g. employment, housing, credit). Reframing Article 22(1) as an exhaustive list of permitted cases risks weakening that protective logic, creating the impression that automated decision-making is generally allowed whenever it falls within one of the listed grounds. To preserve the high level of protection intended by the GDPR, the provision should clearly maintain the formulation that such decisions "shall not" be based solely on automated processing unless specific, strictly defined conditions are met.

The practical implications of this amendment could be far-reaching, as algorithmically-facilitated contract relationships are very common, covering employment, housing, insurance, loans, and many public services. It risks weakening data protection, equality, non-discrimination, and access to effective remedies. Article 22 has been widely recognised in academic literature and

[6] Judgment of the Court of Justice of 7 December 2023, C-634/21, SCHUFA Holding, ECLI:EU:C:2023:957, para. 52

policy recommendations[7] as a central tool to contest algorithmically enabled rights violations. It has also been invoked by digital rights defenders, including notably civil society organisations[8], to challenge the legality and legitimacy of rights-infringing automated systems. Expanding the contractual derogation could normalise automated rejection and decision-making in precisely those domains where individuals are most vulnerable to bias and exclusion, without requiring companies to demonstrate that automation is genuinely necessary. Vulnerable groups who already face discrimination and are at higher risk of human rights violations could be disproportionately affected by potentially harmful algorithms, unchecked by the essential guardrails that human oversight provides.

We therefore recommend preserving the necessity-based limitation in Article 22 GDPR and maintaining its character as a prohibition with narrowly tailored exceptions, in line with the position expressed by the EDPB and EDPS. Fully automated decisions producing significant effects should remain exceptional, and meaningful human oversight must continue to operate as an essential safeguard against discriminatory or otherwise rights-infringing outcomes.

Disclaimer: co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

[7] See for example, S. Wachter, B. Mittelstadt and L. Floridi, *'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR'* (2017) 7(2) *IDPL* 76, p.88–94; E. Bayamlıoğlu, 'The Right to Contest Automated Decisions under the GDPR' (2021) *Regulation & Governance;* Article 29 Working Party (endorsed by EDPB), *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251 rev.01 (2018), p.19–25; EPRS, *Understanding Algorithmic Decision-Making: Opportunities and Challenges* (2020); BEUC (European Consumer Organisation) – *Automated decision-making and artificial intelligence – A consumer perspective*

[8] See for example, NOYB, *'GDPR complaint: Airbnb hosts at the mercy of algorithms'* (22 December 2021); Worker Info Exchange, *'Dutch & UK courts order Uber to reinstate 'robo-fired' drivers'* (14 April 2021)

Co-funded by the European Union