NATIONAL COUNCIL
OF ATTORNEYS-AT-LAW

This document concerns two draft regulations: the Digital Omnibus and the Digital Omnibus on AI.

Digital Omnibus

Analysis of Selected Aspects

Warsaw, February 2026

Analysis of Selected Aspects of the Draft Legislative Package: Digital Omnibus and Digital Omnibus on AI

NATIONAL COUNCIL
OF ATTORNEYS-AT-LAW

Warsaw, 10 February 2026

Table of Contents

I. Subject and Scope of Analysis

The purpose of this paper is to set out selected observations, reservations and proposed amendments concerning certain draft amending Regulations forming part of the Digital Omnibus and Digital Omnibus on AI package presented by the European Commission on 19 November 2025.

This paper has been prepared by the following experts of the New Technologies Committee of the National Bar Council of Attorneys-at-Law:

- Dr hab. Dominik Lubasz, Attorney-at-Law
- Dr Michał Araszkiewicz, Attorney-at-Law
- Anna Augustyn, Attorney-at-Law

This paper does not purport to provide a comprehensive analysis of the draft Regulations included in the Digital Omnibus and Digital Omnibus on AI package, nor does it address all identified issues, interpretative uncertainties or potential solutions. The comments, conclusions and proposals set out herein reflect the discussions and deliberations of the above-mentioned experts.

At the outset, the authors wish to emphasise their support for the adoption of appropriate legislative measures conducive to technological innovation, including the development of artificial intelligence. They consider such measures to be a necessary condition for safeguarding and enhancing the economic competitiveness of the European Union. At the same time, the promotion of innovation must not take place at the expense of the protection of fundamental rights, legal certainty or the accountability of operators active in the AI market. The anticipated benefits of the proposed regulatory amendments should demonstrably outweigh the potential risks, including the weakening of existing safeguards.

In the authors' assessment, certain amendments proposed under the Digital Omnibus package give rise to justified concerns as to whether this balance is adequately preserved. Moreover, some of the proposed solutions raise significant reservations from the perspective of the principles of sound legislative drafting.

Taking into account the role of the self-government of attorneys-at-law as a profession of public trust entrusted with the protection of individual rights and the public interest, it is necessary to draw attention to the practical implications of the proposed amendments.

Attorneys-at-law have direct exposure to regulatory frameworks governing artificial intelligence: both within the scope of their own professional practice (including the implementation and use of AI tools in legal practice) and in the provision of legal services to entities developing and using AI systems, including supporting organisations in ensuring compliance with applicable law, as well as acting as representatives of individuals whose rights may be infringed as a result of the operation of such systems.

For these reasons, legal certainty — including the predictability of the timeline for the application of obligations under the AIA — regulatory transparency, and the preservation of effective mechanisms for the protection of fundamental rights are of key importance. These elements condition, inter alia, the effective judicial protection of natural persons and the proper functioning of the justice system

II. Glossary

Sources of Law	
AIA, AI Act or Regulation 2024/1689	REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)
GDPR or Regulation 2016/679	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, 4.5.2016)
Digital Omnibus	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, and Directives 2002/58/EC, (EU) 2022/2555, (EU) 2022/2557 as regards the simplification of the digital legal framework and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Law Omnibus Act), COM(2025) 837 final

Digital Omnibus on AI	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (AI Digital Law Omnibus Act), COM(2025) 836 final
TFEU	Treaty on the Functioning of the European Union (consolidated version OJ L 326)
Other abbreviations	
FRIA	Fundamental Rights Impact Assessment
GPAI	General Purpose AI
LIA	Legitimate Interest Assessment
AI system	Artificial Intelligence System
ECHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
CJ/CJEU	Court of Justice / Court of Justice of the European Union (from the date of entry into force of the Treaty of Lisbon, i.e., 1 December 2009)

III. General Remarks

1. Consolidation of Data Economy Regulation

The inclusion and consolidation of several digital regulatory instruments – namely the Data Governance Act, Regulation (EU) 2018/1807 on the free flow of non-personal data, Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services, and Directive (EU) 2019/1024 on open data and the re-use of public sector information – within the framework of the Data Act constitutes a delayed, yet directionally appropriate, legislative step. The current regulatory landscape, characterised by the fragmentation of legal instruments and the absence of sufficiently clear cross-references and systemic coordination, is difficult to justify from the perspective of effectiveness, legal certainty and the overall coherence of Union law.

2. Central Thesis Regarding Regulatory Fragmentation

The Artificial Intelligence Act should not be considered the main regulatory obstacle for undertakings. The primary challenge remains regulatory fragmentation and the overlapping scope of multiple Union instruments, which increases compliance complexity and legal uncertainty for market participants.

3. General Objective of Simplification

The overarching objective of both the Digital Omnibus on AI and the Digital Omnibus package – namely to simplify the regulatory framework and reduce unnecessary administrative burdens – merits a positive assessment. In this regard, the authors concur with the position expressed by the EDPB and the EDPS in Joint Opinion 1/2026, in which those bodies support efforts aimed at facilitating the effective implementation of the Artificial Intelligence Act and alleviating administrative burdens, provided that such simplification does not result in a lowering of the level of protection of the fundamental rights of natural persons, in particular the right to the protection of personal data. Proposals such as the establishment of a single point of contact, the development of a common template and harmonised methodology for conducting data protection impact assessments, or amendments to the regulatory framework governing the use of cookies, should be viewed favourably.

4. Cooperation between the AI Office and National Authorities

The requirement to ensure active and structured cooperation between the AI Office and national competent authorities in the supervision of AI systems based on general-purpose AI (GPAI) models also merits a positive assessment. Greater centralisation of supervisory competences with regard to specific categories of AI systems may contribute to the consistent application and enforcement of the Artificial Intelligence Act at Union level.

5. Social and Institutional Criticism

While the overarching deregulatory objective of the Digital Omnibus packages may be viewed positively, a substantial number of the detailed proposed amendments give rise to serious reservations regarding the preservation of fundamental rights and freedoms.
It should be noted that the proposals have been subject to unprecedented criticism. Over 120 civil society organisations issued an open letter characterising the measures as "the largest rollback of digital rights in EU history." Criticism has also been expressed by prominent organisations, including European Digital Rights (EDRi) and NOYB, as well as by academic institutions and think-tanks.

IV. Detailed Remarks

1. Changes to the GDPR (Regulation 2016/679)

1.1. Detailed remarks

1.1.1. Assessment of the General Direction of the Proposed Amendments

The proposed amendments to the General Data Protection Regulation, notwithstanding the declared objective of simplifying the regulatory framework and enhancing the competitiveness of the European digital economy, give rise to serious concerns from the perspective of the protection of fundamental rights and the coherence of the Union legal order. Efforts aimed at facilitating the implementation of AI systems and reducing administrative burdens merit support. However, such simplification must remain conditional upon maintaining a high level of protection of the fundamental rights of natural persons, in particular the right to the protection of personal data enshrined in Article 8 of the Charter of Fundamental Rights of the European Union.

1.1.2. Risk of Undermining the Principle of Technological Neutrality

The proposed Article 88c of the General Data Protection Regulation, which would recognise the development of AI systems as a legitimate interest within the meaning of Article 6(1)(f) GDPR, gives rise to fundamental reservations in light of the principle of technological neutrality. To date, Article 6(1) GDPR has been framed in technologically neutral terms. Under the proposed amendment, for the first time, a specific technology — rather than a processing purpose or legal ground — would be expressly legitimised within the structure of lawful processing. Such an approach risks implying that processing operations are lawful merely because AI technology is used, whereas comparable processing activities carried out without reliance on AI might not fall within the scope of Article 6(1)(f) GDPR. This constitutes a breach of a fundamental principle on which European data protection law is founded. Similarly, the principle of technological neutrality would be undermined by the proposed amendment to Article 9(2) GDPR introducing point (k).

1.1.3. Redundancy of Legislative Intervention

The position concerning the possibility of relying on legitimate interest as a legal basis for the development of AI systems is, in essence, consistent with what has already been articulated by the EDPB in Opinion 28/2024 on the processing of personal data in the context of AI models. That Opinion acknowledges that the development of AI systems may, in principle, be based on Article 6(1)(f) of the General Data Protection Regulation, provided that strict safeguards are respected. Given that an interpretative position has already been formulated, the necessity and purposefulness of legislative intervention may legitimately be questioned. The proper application of the existing legal framework by supervisory authorities and the EDPB, appears sufficient, without the need to amend the substantive provisions of the GDPR. The interpretation of the law falls within the competence of the bodies responsible for its application, rather than the legislator. Similar reservations arise in relation to the proposed amendment concerning the concept of personal data, which, in our view, is not only redundant but may also significantly narrow the scope of application of the GDPR, as discussed in greater detail in the specific comments below.

1.1.4. Alternative Regulatory Approach

The GDPR already provides adequate and flexible regulatory mechanisms, in particular through the broad normative scope of the data processing principles and the procedural, risk-based approach embedded in its structure. Greater potential for ensuring effective protection of fundamental rights, while at the same time fostering innovation, lies not in further legislative amendments to the GDPR, but in alternative measures. In the short term, consideration should be given in particular to:

– the adoption by the EDPB of guidelines pursuant to Article 70(1)(e) GDPR addressing issues such as transparency in AI systems, the right to object to the processing of training data, purpose limitation in the context of AI training, and appropriate safeguards within the meaning of Article 10(5) of the AIA;
– the establishment of regulatory sandboxes in accordance with Article 57(1) and (2) of the AIA;
– the strengthening of supervisory authorities through the creation of specialised structures dedicated to AI-related matters; and
– the effective enforcement of Regulation (EU) 2025/2518 of 26 November 2025 establishing additional procedural rules for the enforcement of Regulation (EU) 2016/679.

1.2. Detailed Remarks

1.2.1. Amendment to the Definition of Personal Data (Article 4(1) GDPR)

a) Distortion of the Logic of Recital 26 GDPR

The proposal alters the logic of Recital 26 of the GDPR by transferring fragments of that recital into the operative provisions, while distorting their meaning and context. Recital 26 GDPR constituted an interpretative exception, narrowly confined to situations in which a natural person is not identifiable in a manner reasonably likely, taking into account all entities that may reasonably have access to means of identification. The proposal transfers to Article 4(1) only a "cut-out fragment" of that recital, but omits the element requiring an assessment of all means reasonably likely to be used, omits the requirement to assess the technological, economic and infrastructural context, and omits the risk of identification by other actors within the data ecosystem. Identification is not solely a characteristic of the data themselves, but of the ecosystem in which the data are processed — a dimension that the proposal fails to take into account, thereby resulting in an erroneous and partial narrowing of the definition of personal data.

b) Deformation of the Meaning of Recital 26 GDPR

The proposal alters the meaning of Recital 26 of the GDPR by replacing a risk-based assessment of identifiability with an analysis confined to the perspective of a single entity. Recital 26 requires an assessment of all means reasonably likely to be used for identification, taking into account all parties that may obtain access to the data, the costs and time required for identification, available technologies and technological developments. By contrast, the Commission's proposal appears to reduce this assessment to the question whether a specific entity is capable of identifying the person concerned. This constitutes a fundamental shift, leading to an excessive relativisation of the notion of personal data to the resources of a given controller, rather than to the actual risk of interference with the rights and freedoms of natural persons and to contextually objective criteria relating to the data ecosystem. Such an approach further accentuates the subjectivisation of the concept of personal data, thereby significantly narrowing its scope.

c) Uncontrolled Erosion of the Definition

The transfer of a fragment of Recital 26 into Article 4 creates an uncontrolled erosion of the definition of personal data. Recitals are interpretative instruments, not normative

ones. Their incorporation into a law-creating provision turns an exception into a rule, elevates interpretation to the rank of a norm, and alters the structure of data protection contrary to the construction of the GDPR. Recitals perform a dynamic function, adapting to the case-law of the Court of Justice of the European Union. Replacing them with a binding provision blocks that flexibility and leads to overregulation in a direction favourable to controllers.

d) Disregard for the CJEU Acquis

The proposed amendment appears to disregard the acquis of the CJEU, of which Recital 26 of the GDPR constitutes a reflection. In its judgments in Breyer v Bundesrepublik Deutschland, Nowak v Data Protection Commissioner and Jehovan todistajat, the Court developed the criterion of relative identifiability, taking into account contextual elements and the realistic possibility of identification. That approach was subsequently reflected in Recital 26 GDPR. By limiting identifiability to the perspective of a single entity, the Commission's proposal risks disrupting the coherence between Recital 26 and Article 4 GDPR and introducing a new, formalistic definition that departs from the material risk-based assessment applied in the Court's case-law. Such an approach weakens the role of judicial interpretation in shaping the concept of personal data and leads to a "freezing" of the legal framework at a time when identification algorithms are developing dynamically.

e) Limitation of the Scope of GDPR Application Contrary to Its Objectives

The proposed amendment may limit the scope of application of the GDPR in a manner inconsistent with its objectives (Article 1, Recital 4). The definition of personal data constitutes the gateway for the application of the entire data protection framework. The proposed change significantly narrows this concept, contrary to the objectives of the Regulation and established CJEU case-law, by aprioristically restricting its applicability to specific subjects. This approach conflicts with the fundamental contextuality of the Regulation and its risk-based methodology. As a result, the amendment may reduce the scope of GDPR application, enabling controllers to assert that they "do not possess means of identification," and may facilitate commercial grouping, profiling, or analysis of data that is classified as allegedly "non-personal." In AI and big data environments, such data can be automatically reproduced, reconstructed, or correlated with other datasets, meaning that the risk of identification remains real.

f) Favouring Market Interests at the Expense of Individual Protection

The amendment favours controllers and market interests at the expense of the protection of individuals. The proposal explicitly facilitates: the use of pseudonymised data as allegedly non-personal data; the transfer of data to third parties without GDPR obligations; the exclusion of information obligations towards data subjects; and the conduct of analysis and the training of AI models without oversight. This appears to be the result of business and political pressure rather than legal necessity. Recital 26 was a protective instrument, not a tool for deregulation.

g) Inconsistency with the Precautionary Principle Regarding AI Risks

The amendment places the GDPR in contradiction with the precautionary principle in relation to AI-related risks. In the context of AI, the definition of personal data should be interpreted broadly and in a pro persona manner, because data that were originally "anonymous" may be easily re-identified; aggregated data may contain information about individuals; identification may be probabilistic and algorithmic; and the data ecosystem is global rather than confined to an "administrator-silo" model. The proposed amendment ignores these processes and entrenches a definition that is inadequate in light of AI-related risks.

h) Lack of Impact Assessment for the Protection of Human Rights and Freedoms

The proposed amendment lacks a thorough impact assessment with regard to the protection of fundamental rights and freedoms. The Commission has not presented an analysis of the potential effects on fundamental rights (Articles 7–8 of the Charter of Fundamental Rights of the European Union), nor an assessment of the systemic risk of identification in AI, or of the impact on decision-making processes in public administration, finance, health, and education. The absence of such analyses is particularly concerning given that Recital 26 was designed to support a risk-based assessment, whereas the proposal almost entirely removes the evaluative and contextual dimension.

1.2.2. Changes to the Principle of Purpose Limitation (Article 5(1)(b) GDPR)

Although Article 5(1)(b) GDPR, in its current wording, provides for a presumption of compatibility of further processing for scientific purposes, the protection of the rights of individuals – as reflected in Recital 159 GDPR – requires an individual assessment of proportionality, necessity, and risk, carried out in accordance with Article 89(1) GDPR.

The proposed amendment, by excluding the application of Article 6(4) GDPR, removes a crucial component of this assessment, thereby simplifying the process at the expense of both the level of data protection and the systemic consistency of the Regulation. This amendment does not follow from the logic of the GDPR nor from the CJEU case-law, but rather constitutes a deregulatory procedure of a political-economic nature, as is also evident from Recital 29 of the proposal.

a) Risk of Excluding the Compatibility Test of Purposes

The proposed amendment, similarly to the addition of a definition of "scientific research," may create a risk that the obligation to perform the compatibility test under Article 6(4) GDPR is no longer applied. This test constitutes a fundamental component of the data protection framework, ensuring that further processing of personal data remains consistent with the purposes for which the data were originally collected, or is otherwise compatible with those purposes in light of the legitimate expectations of the data subjects.

b) Issue of the Lack of a Legal Definition of Scientific Research

The GDPR does not provide a legal definition of the concept of "scientific research." At the same time, referring to Recital 159 GDPR, it should be emphasised that the concept must be interpreted in accordance with its common meaning and understanding. Accordingly, "scientific research" should be understood as a research project conducted in accordance with appropriate sectoral methodological and ethical standards, and in compliance with good practice. This encompasses systematic activities, including the collection and analysis of data, which contribute to the accumulation of knowledge and understanding and to their practical application. It is important to note that commercial research is not excluded from this concept; however, the purpose of research is understood as the generation of knowledge, which in turn may improve the quality of life of individuals and enhance the efficiency of social services.

c) Restriction on Further Use of Research Results

Further use of personal data should be possible with regard to the results of research, rather than the underlying data on which the research was conducted. The proposed amendment does not take this fundamental distinction into account, which may allow unlimited secondary use of raw personal data under the pretext of "scientific research."

d) Normativisation of Recital 159 GDPR

The introduction of a definition of "scientific research," similarly to the partial transposition of Recital 26 into Article 4(1), constitutes a normativisation of Recital 159 GDPR. It should again be emphasised that recitals are interpretative tools, not normative provisions. Incorporating them into a law-making article elevates an interpretation to the rank of a norm, limits contextual flexibility and the dynamic meaning of the recitals – which, in the context of the technological neutrality of the GDPR, is highly significant, particularly in light of CJEU case-law. Replacing recitals with a provision blocks this flexibility and leads to over-regulation in a manner favourable to controllers. The significance of recitals is strongly context-dependent, and the concepts they contain are to be interpreted through the lens of EU regulatory principles and directives. In the EU context, this particularly includes the principles of trustworthy artificial intelligence, which serve as a point of reference and condition the interpretation – also of GDPR provisions – including those concerning the concept of scientific research, while taking into account the protective objectives of the GDPR.

e) Extension of the Concept of Scientific Research to Commercial Purposes

The concept of "scientific research" is, contrary to the original intent of the legislator as expressed in Recital 159 GDPR, extended to activities carried out primarily for commercial purposes. Given the specificities of the AI lifecycle, this effectively implies that the training phase of any AI system could fall within the scope of "scientific research." This represents a fundamental distortion of the research exception, which was intended to promote the advancement of knowledge in the public interest, rather than to facilitate the commercial exploitation of personal data.

1.2.3. Processing of Special Categories of Data in the Context of AI (Articles 9(2)(k) and 9(5) GDPR)

The structure of the proposed Articles 9(2)(k) and 9(5) GDPR, which address the processing of special categories of personal data in the development and operation of AI systems, is flawed for multiple systemic and practical reasons.

a) Overturning the Article 9 GDPR System

The introduction of a new legal basis for the processing of special categories of personal data overturns the structure of Article 9 GDPR. Article 9 GDPR is built on a highly exceptional model: the general rule is a total prohibition on processing special

categories of data, with exceptions exhaustively listed and narrowly defined, and each exception must be interpreted strictly and restrictively. The addition of point (k) ("AI system or AI model") expands the catalogue of exceptions in a manner that is systemically inconsistent, detached from the logic of protecting special categories of personal data, and oriented toward technological interests rather than protective ones. As the CJEU has indicated, any interference must meet the criteria of necessity and proportionality, so as not to affect fundamental rights in an undifferentiated or general manner – requirements that the proposal does not appear to satisfy (see, inter alia, C-293/12 and C-594/12, Digital Rights Ireland, paras. 52–54).

b) Extremely Broad Scope of the Exception

The scope of the proposed exception is extremely broad and effectively encompasses nearly all stages of the AI system lifecycle. The provision applies to the training, testing, validation, and operation of AI models. As a result, the exception does not relate to a "specific activity" but to the entire lifecycle of an AI model. Any processing of special categories of data within AI systems – including commercial, mass-scale, or otherwise unverifiable processing – could therefore be considered lawful. This is highly concerning, as no other exception under Article 9(2) GDPR has such a general structure.

c) Lack of Requirement for Necessity and Proportionality

The proposed provision does not require demonstrating necessity or proportionality. Point (k) omits two fundamental protective conditions present in most other exceptions: the necessity of processing and proportionality in light of the purpose pursued. Most exceptions under Article 9(2) concern public health, the saving of lives, employment, the protection of important public interests, archival purposes in the public interest, or scientific, historical, or statistical research. By contrast, point (k) permits the processing of special categories of data on the basis of the technical or developmental interest of a private controller. This fundamentally disrupts the value framework of the GDPR.

d) Lack of Determination of the Purpose Justifying Processing

Article 9(2)(k) does not specify a purpose that justifies the processing of special categories of personal data. The exceptions under Article 9(2) are strictly linked to material purposes such as health protection, labour law, or important public interests. Point (k), by contrast, does not indicate any concrete, material purpose, merely referring to "processing in the context of the development and operation of an AI system." Such broad wording effectively legalises almost any AI model, removes the requirement to

demonstrate a public interest, and eliminates the distinction between private and public interests. Consequently, entities developing commercial technologies could process sensitive data for their models just as easily as research units acting in the public interest – a result contrary to the fundamental value framework of the GDPR.

e) Technical Unreality of Article 9(5)

The provision assumes that sensitive data can be removed "if they are detected," which is technically unrealistic. Article 9(5) GDPR requires the identification of sensitive data within datasets, followed by their removal or protection. Practical problems arise: AI cannot detect all sensitive data, particularly inferred data; in machine learning models, sensitive data may be embedded in model parameters and thus be irretrievable; removing the data does not eliminate the information encoded in the model weights; controllers lack the means to verify whether the model continues to "remember" sensitive data; and "machine unlearning" mechanisms remain largely experimental. Consequently, the provision relies on a technical fiction.

f) Loophole for Bypassing Consent

The exception in point (k) will be exploited as a loophole to circumvent the consent requirement under Article 9(2)(a) GDPR. In the AI context, most processing of special categories of data should rely on specific consent (Article 9(2)(a)) or fall within other public-interest-based exceptions (points g–j). Point (k) will enable controllers to avoid obtaining consent or fulfilling other lawful bases for processing special categories of data.

g) Lack of Distinction Between Development and Operation Phases

The provision does not establish a detailed distinction between exploratory processing (development) and operational processing (operation), applying the same legal basis to both phases and disregarding differences in the potential level of impact of processing on the rights and freedoms of data subjects.

h) Appropriate Place of Regulation

The appropriate regulatory framework for the processing of special categories of data for the purposes of bias detection and correction is Article 10(5) of the AIA. This regulation should remain in that provision, with any possible extension of the scope with respect to entities and activities strictly limited It is justified to maintain the "strict

necessity" standard currently applied to high-risk AI systems for all providers and entities implementing AI systems with respect to the processing of special categories of personal data, notwithstanding the differences in the scope of application of the GDPR and the AIA.

1.2.4. Information Obligations (Article 13 GDPR)

The proposal to exempt controllers from full information obligations where they consider the relationship with the data subject to be "clear and circumscribed," or where they believe that the individual already has the relevant information, raises serious concerns.
It should be emphasised that **Article 13(4) GDPR already provides for a limited exception**: paragraphs 1, 2, and 3 do not apply to the extent that the data subject already has the information. The proposed amendment, however, goes significantly further, introducing additional discretionary criteria for excluding the information obligation.
In practice, this could render transparency optional: data subjects would no longer be clearly informed about what data is collected, for what purpose, or for how long it is stored. Without this knowledge, rights such as access, objection, or erasure lose practical effect, as individuals may be unaware that they can exercise them. The proposed extension of exclusions therefore constitutes a substantial weakening of the fundamental principle of transparency, which is a sine qua non for effective personal data protection.

1.2.5. Automated Decision-Making (Article 22 GDPR)

The proposed amendment to Article 22 GDPR, which replaces the current prohibition with a conditional allowance and removes the requirement of "necessity" as a condition for the lawfulness of automated decision-making in a contractual context, constitutes a fundamental shift in regulatory philosophy. Article 22 was intended to serve as a strong protective mechanism, ensuring the autonomy of data subjects and their ability to exercise oversight.

a) Change in the Philosophy of Data Protection — From Prohibition to Permission

Article 22, in its current form, is grounded in the principles of protection against automation, safeguarding individual autonomy, ensuring minimum human control, and applying a precautionary approach to automated decision-making. The Digital Omnibus, by contrast, shifts this philosophy towards normalising automated decision-making,

enabling its mass deployment, and effectively allowing decisions to be taken without prior human involvement.

b) Practical Significance of Removing the Necessity Requirement

Until now, automated decision-making in contractual contexts could only be employed when its absence made the performance of the contract impossible. For example, credit scoring based solely on automated decision-making could only be applied if the bank had no feasible alternative. Following the proposed amendment, the controller may choose to use automated decision-making independently, without demonstrating that it is necessary for the conclusion or performance of the contract. Consequently, automated decision-making becomes a business option for the controller rather than an exception designed to protect the data subject. This represents a complete reversal of the prior regulatory logic.

c) Automated Decision-Making as a Business Standard

In numerous sectors – including banking, insurance, telecommunications, employment, health, education, and media – controllers will be allowed to adopt automated decision-making as the default. They may justify it as "efficient," "cheaper," or "faster," reduce manual oversight, and delegate high-stakes decisions to algorithms. This regulatory change therefore constitutes a paradigm shift.

d) Loss of Possibility of Real Choice by the Data Subject

Without the necessity requirement, data subjects cannot demand an alternative. Controllers may refuse to provide a service if automated decision-making is declined, and market practices are likely to compel consent to automated decision-making as a condition for accessing most services. This results in a form of algorithmic economic coercion.

e) Illusory Nature of the Right to Human Intervention

The right to human intervention under Article 22(3) becomes illusory. If automated decision-making is permitted without restrictions, human intervention occurs only post factum. The decision-making process is then fully automated, and the human role is effectively reduced to "explaining the decision" rather than actively making it – contrary to the protective intent of the current regulation.

f) Conflict with CJEU Case-Law

The CJEU, in cases C-634/21 SCHUFA and C-184/20 Vyriausioji tarnybinės etikos komisija, has emphasised that any deviations from or limitations of the principle of protecting special categories of data must be applied strictly within the bounds of necessity. Automated decision-making must be strictly limited, the necessity test is decisive, and balancing the asymmetry between the controller and the data subject is essential. The Digital Omnibus proposals disregard this established line of case-law.

1.2.6. Legitimate Interest for AI Systems (Article 88c GDPR)

The proposed Article 88c GDPR raises numerous practical and systemic issues that extend beyond the question of technological neutrality.

a) Systemic Weakening of Personal Data Protection

Article 88c GDPR creates a sectoral exception for AI technologies, extending the scope of permissible data processing, including secondary processing. It privileges the controller's interest over the rights of the individual, detaches the controller's interest from the requirement of necessity and legal justification – reducing it to a mere declaration – and establishes legitimate interest as the default mechanism. As a result, the rights and freedoms of the data subject become the exception rather than the objective of protection. This reverses the value framework of the GDPR, whose primary goal is the protection of fundamental rights, not the support of technological development, in the absence of a hierarchy of legal bases for processing. The provision introduces a strictly technological exception into a framework intended to remain technologically neutral.

b) Contradiction with EDPB Opinion 28/2024

EDPB Opinion 28/2024 does not justify privileging legitimate interest for AI. On the contrary, it emphasises: the absence of a hierarchy of legal bases, the necessity of a complete legitimate interest assessment (interest – necessity – balance), the special risks associated with AI models, and the lack of reasonable expectations by data subjects regarding the use of their data for AI training. Article 88c disregards these requirements, creating a "statutory simplification" that is contrary to the guidance of the EDPB.

c) Conflict with CJEU Case-Law

The CJEU requires strict interpretation of exceptions, consideration of context and information asymmetry, and special protection against profiling. Article 88c permits processing during both the development and operation of AI models without a necessity test, without assessing purpose compatibility, and in conditions of extreme knowledge asymmetry between the controller and the data subject. This contravenes established case-law, including Meta, SCHUFA, Nowak, and Jehovan todistajat. According to CJEU jurisprudence (C-252/21 Bundeskartellamt, para. 112; C-621/22 Tennisbond, para. 55), the reasonable expectations of data subjects are central to the assessment of the balance of interests. In AI training and operations, the complexity, multiplicity, and continuous evolution of systems mean that data subjects cannot reasonably anticipate such processing or its scope.

d) Violation of Key GDPR Principles

Purpose Limitation (Art. 5(1)(b)) – Article 88c enables secondary processing of personal data for AI purposes without conducting the compatibility assessment required under Article 6(4) GDPR. This effectively places such processing outside the general framework governing further processing and relies solely on Article 6(1)(f). Data Minimisation (Art. 5(1)(c)) – AI models require large-scale and diverse datasets; Article 88c does not provide for genuine or effective minimisation mechanisms. Accountability (Art. 5(2)) – Shifting the assessment of lawfulness to the controller's mere declaration of the existence of an "interest," without requiring a demonstration of necessity or proportionality, weakens the principle of accountability. Right to Object (Art. 21) – In practice, this right becomes ineffective, as data used to train AI models are not subject to reversible removal.

2. Changes in the AIA (Regulation 2024/1689)

2.1. General Remarks

2.1.1. Assessment of the General Direction of Changes

The declared objectives of the Digital Omnibus on AI proposal include, inter alia, simplifying the application of the AIA and reducing administrative burdens for enterprises. As such, these objectives deserve approval. It should be borne in mind,

however, that in practice many of the proposed amendments do not appear to be merely technical, organisational, or "clarificatory" in nature. More importantly, some of them may entail a serious risk of undermining mechanisms designed to protect fundamental rights, ensure accountability, and safeguard the effective enforceability of obligations imposed on providers and deployers. In the longer term, they may even lead to systemic deregulation.

2.1.2. Processing of the Proposal

The Digital Omnibus on AI proposal is being processed at an exceptionally accelerated pace, which raises serious concerns regarding both the completeness of the European Commission's assessment of the regulation's effects and the adequacy of public consultation. Documents made public by Corporate Europe Observatory indicate that preparatory consultations, known as "Reality Checks," were attended predominantly by business representatives. For instance, the "Reality Check on AI" involved ten companies and industry associations — including actors advocating for a weakening of the AIA — and only two civil society organisations. Given the substantial economic, legal, and social impact of AI, regulatory changes of this magnitude should be preceded by broad and balanced consultations, ensuring proportionate representation of all relevant stakeholders, including public authorities, academia, consumer organisations, human rights bodies, and civil society.

2.1.3. Impact on Fundamental Rights

From a systemic perspective, the proposed amendments to the AIA appear to weaken – or at least create a real risk of weakening – the mechanisms designed to protect fundamental rights as established in the original regulation.
While individual amendments to the AIA may, in principle, provide justified regulatory simplifications (and may indeed do so in practice), the absence of a comprehensive impact assessment, the accelerated pace of processing, and insufficient representation of stakeholders outside the industrial sector prevent a reliable evaluation of the proposal's actual effects on fundamental rights and the risks these changes may entail. An analysis of the individual amendments in their mutual interaction indicates a general risk of systemic weakening of fundamental rights protection mechanisms.

2.2. Detailed Remarks

2.2.1. Change of the Application Schedule (Articles 111 and 113 AIA)

The AIA currently provides for the application of provisions concerning high-risk AI systems from 2 August 2026 (Annex III — including biometric systems, justice, education, employment, and migration) and from 2 August 2027 (Annex I — including medical devices, aviation, and toys).
Article 111(2) AIA establishes a transitional mechanism, commonly referred to as a "grandfathering" clause, according to which high-risk AI systems placed on the market or put into service before 2 August 2026 are, as a rule, exempt from the obligations set out in the regulation, in order to prevent retroactive application. These obligations will apply only if the system undergoes significant design changes after this date. A separate adjustment period is established for high-risk AI systems intended for use by public authorities, requiring providers and deployers to ensure compliance with regulatory requirements no later than 2 August 2030.
The Digital Omnibus on AI proposal introduces a modification to the application schedule through a so-called "stop-the-clock" mechanism, i.e., a conditional deferral of application dependent on the European Commission confirming the availability of compliance support tools. Under this mechanism, the deadline would be extended no later than 2 December 2027 for systems from Annex III and 2 August 2028 for systems from Annex I.

By deferring the application of Chapter III provisions for high-risk systems listed in Annex III (Art. 6(2)), the proposal effectively extends the transitional period provided by the grandfathering mechanism in Article 111(2) – shifting the deadline from 2 August 2026 to a maximum of 2 December 2027. As a result, a greater number of high-risk AI systems from Annex III could operate on the market for a longer period without full compliance with Chapter III obligations.

a) Impact on Justice and Public Administration

Deferring the application of Chapter III provisions for high-risk systems from Annex III would mean that, until 2 December 2027, AI systems used in justice, law enforcement, and public administration – areas with potentially significant effects on individual rights – could operate de facto without complying with key requirements of the chapter. These include: Full risk management obligations (Art. 9), data and data governance requirements (Art. 10), obligations to ensure human oversight (Art. 14), transparency

requirements and the provision of information to deployers (Art. 13), deployers' obligations, including conducting fundamental rights impact assessments (Arts. 26–27).

b) Threat to the Protection of Fundamental Rights

The proposed delay in applying key Chapter III provisions implies that, for up to an additional 16 months, AI systems potentially exerting a significant impact on human rights could operate without the full protective framework of Chapter III. This is particularly relevant for systems used in biometrics, justice, law enforcement, migration, education, and employment – sectors where the risk of infringing fundamental rights is especially high.

It should be emphasised that this deferral does not imply a total absence of legal safeguards. For instance, the GDPR and other EU fundamental rights standards, including the Charter of Fundamental Rights, continue to apply. However, these frameworks do not generally address AI-specific risks, which the AIA was designed to manage. The AIA introduces dedicated protective mechanisms beyond existing standards, including requirements on the quality of training data, obligations to ensure human oversight, and fundamental rights impact assessments specific to AI systems.

c) Context of the Lack of Technical Standards and the "Stop-the-Clock" Mechanism

The proposal justifies the introduction of the "stop-the-clock" or "moving deadline" mechanism for high-risk AI systems by arguing that delays in preparing compliance support instruments — in particular harmonised standards, common specifications, and guidelines — could hinder the practical implementation of obligations and increase compliance costs. In the Commission's assessment, this is presented as a rationale for departing from the original application date of 2 August 2026.
While this rationale is partially justifiable, from the perspective of fundamental rights protection and legal certainty it must be emphasised that many obligations under Chapter III are organisational and procedural in nature (e.g., risk management systems, human oversight, and record-keeping) and can be implemented independently of a complete set of harmonised standards. Consequently, delays in standardisation alone should not automatically justify deferring the application of the entirety of Chapter III (Sections 1–3).

Furthermore, the conditional and difficult-to-predict timing of the Commission's decision complicates compliance for providers and deployers of AI systems and makes

it more challenging for competent authorities to prepare for supervision and enforcement of the provisions.

d) Postulate of Differentiating Obligations

It appears justified to consider differentiating the deferral according to the type of obligations. In particular, obligations that are not directly dependent on technical standards – for example, transparency obligations towards deployers, the basic elements of the risk management system, human oversight, and organisational requirements on the part of deployers, including preparation for the FRIA – could be applied according to the original schedule or with a shorter deferral, while a longer period could be reserved exclusively for strictly technical requirements.

e) Backstop Dates

The introduction of so-called backstop dates –2 December 2027 for Annex III and 2 August 2028 for Annex I – should be assessed positively. These dates ensure a minimum level of predictability, indicating the latest moment at which the provisions will apply irrespective of the Commission's decision. However, they do not eliminate legal uncertainty in the period preceding these dates, as obligated entities still cannot know precisely when the provisions will come into force.

2.2.2. Competences in the Field of AI (Art. 4 AIA)

The Commission's proposal introduces a significant change to Article 4 AIA. Under the current regulation, providers and deployers of AI systems are obliged to ensure that their personnel have, to the greatest extent possible, the appropriate knowledge and competencies. The proposed amendment, however, replaces this obligation with a commitment of Member States and the Commission merely to encourage these entities to take steps to develop the AI competence of their personnel.

Replacing a binding obligation with a mere encouragement primarily undermines the accountability and enforceability of AI literacy standards for providers and deployers of AI systems. It should not be assumed that these standards will be automatically met simply because compliance with other AIA obligations functionally depends on personnel possessing appropriate AI knowledge. Removing AI competence as an independent compliance requirement may result in AI literacy training being treated as a discretionary cost – either omitted entirely or at least deprioritised.

a) Weakening of the Regulation's Objective

The amendment to Article 4 AIA significantly weakens the overarching objective of safe and responsible AI implementation. Without a binding obligation for personnel to have appropriate competencies at every stage of the AI lifecycle, the level of protection of fundamental rights – including the right to data protection – may be directly reduced. This concern is echoed by the EDPB and the European EDPS in their joint opinion 1/2026.

b) Problem of Ambiguity and Proportionality

Both the current and proposed wording of Article 4 AIA raise interpretative doubts due to the use of undefined concepts, in particular the notion of a "sufficient level," which in practice may create uncertainty regarding the scope of required measures (for example, the depth, frequency, and verification of training or the assessment of acquired competencies). References to criteria such as "technical knowledge, experience, education and training" and the "context" are evaluative in nature and do not establish minimum standards. Additional uncertainty arises regarding the subjective scope of the provision, namely which employees or collaborators actually require training.

c) Maintenance of Training Requirements for High-Risk Systems

It should be noted that the proposed change does not abolish obligations for deployers of high-risk AI systems. As set out in Article 26(2) AIA, deployers remain obliged to entrust human oversight to natural persons possessing the necessary competence, training and authority, and to ensure appropriate support. However, this normative status may reinforce the perception among providers and deployers that AI literacy standards are less relevant for AI systems that are not classified as high-risk.

d) General Recommendation of EDPB and EDPS

In their joint Opinion 1/2026, the EDPB and EDPS strongly recommend retaining the mandatory character of provisions regarding AI competence. The bodies also call on the European Commission and relevant regulatory authorities to issue practical guidance for providers and deployers on implementing AI literacy, rather than abolishing the existing obligation under Article 4 AIA.

e) Doubts Regarding the Justification of the Change

The justification for the proposed amendment to Article 4, set out in Recital 5, raises doubts as it is based on the assumption that the original obligation was "uniform" in character. The obligation to ensure AI literacy did not imply a rigid, one-size-fits-all standard for all entities. Rather, in accordance with its function and the principle of

proportionality, it allowed for and assumed differentiation in the scope and intensity of training activities depending on the scale of the entity's operations, the type of AI systems, and the context of their use. Moreover, the amendment does not resolve this issue, since the model based on "encouragement" likewise remains normatively undefined and does not introduce any new mechanisms for meaningful differentiation among the addressees. Consequently, the argument of a "one-size-fits-all" obligation appears to serve primarily as a rhetorical justification for weakening the norm rather than as a genuine diagnosis of a defect in its original construction.

2.2.3. Abolition of the Obligation to Register AI Systems (Amendment to Article 6(4) and Repeal of Article 49(2) and Section B of Annex VIII AIA)

The AIA currently allows providers of AI systems listed in Annex III to independently assess whether their system does not constitute a high-risk system, provided that at least one of the conditions set out in Article 6(3) is met (e.g., the system serves a narrow procedural task or improves the result of a previously completed human activity) and it does not create a significant risk of harm to the health, safety, or fundamental rights of natural persons. As a mechanism balancing this freedom of self-assessment, the AIA simultaneously imposes an obligation to register such systems in an EU database (Article 49(2), Section B of Annex VIII). The Digital Omnibus on AI proposes to abolish this registration requirement, leaving only the obligation to document the assessment before placing the system on the market or putting it into service, and to make this documentation available to national authorities upon request.

Abolishing the registration requirement may primarily reduce transparency regarding providers' self-assessments at the ex-ante stage. Consequently, reliable due diligence by deployers and the possibility for competent authorities to react early will depend to a greater extent on ex-post measures, based solely on documentation provided upon request.

a) Removal of the Public Oversight Mechanism

It should be emphasised that the registration obligation constitutes the only form of prior supervision – that is, supervision before a system is placed on the market – over the provider's decision to classify an Annex III system as not being high-risk. Public registration allows deployers of AI systems to conduct appropriate verification and risk assessment before implementation, and enables national authorities and fundamental rights bodies (FRABs) to take supervisory actions before the system enters the market.

The EDPB and EDPS, in Opinion 1/2026, explicitly recommend maintaining this obligation, noting that its abolition would significantly weaken providers' accountability and create an incentive to abuse the exclusion. It should also be noted that any savings for providers are negligible compared to the potential risks to fundamental rights.

b) Transparency and Accountability

Limiting the registration obligation reduces administrative burdens for system providers but significantly weakens the public visibility of classification decisions, shifting key justifications to internal documentation maintained by the provider. As a result, accountability becomes largely conditional and reactive, dependent on the initiative of supervisory authorities rather than on systemic ex-ante transparency. While the obligation to document the risk assessment preserves a minimal standard of control, the absence of disclosure in the register limits the possibility of external verification – both by authorities in other Member States and by other stakeholders. According to Recital 9, access to the documentation would be restricted to the "national competent authorities." This arrangement is not optimal from the perspective of protecting private entities, including attorneys-at-law and their clients.

c) Risk to the Justice System

From the perspective of the self-governing body of attorneys-at-law, as a profession of public trust tasked with providing professional legal assistance, including representing clients before courts, a particularly significant and high-risk consequence of the proposed change is the exclusion of AI systems used in the justice sector from the registration obligation. Given the open and vague nature of the exceptions set out in Article 6(3) AIA, leaving their assessment solely to providers creates risks to fundamental rights, including the right to a fair trial, and to the core principles of the rule of law. These risks are especially critical for the legal protection of participants in proceedings, on whose behalf attorneys-at-law act. Furthermore, potential damage arising from the malfunction of unregistered systems may be practically difficult to remedy, considering the irreversible consequences of certain procedural decisions made using these systems. Maintaining the registration requirement for systems not classified as high-risk would partially mitigate these risks at the ex-ante stage.

2.2.4. Cooperation with Fundamental Rights Protection Bodies (Article 77 AIA)

Pursuant to Article 77 of Regulation (EU) 2024/1689 (AIA), national authorities or public bodies that supervise or enforce compliance with the respect of obligations under Union

law protecting fundamental rights (so-called FRABs – Fundamental Rights Authorities/Bodies) will have the power to request documentation from providers and deployers of high-risk AI systems where access to such documentation is necessary for effectively fulfilling their mandates. According to the Digital Omnibus on AI proposal, such requests for access by FRABs would be made through an intermediary, namely the relevant market surveillance authorities (MSAs).

By way of example, in the national context (pursuant to the draft Act on Artificial Intelligence Systems), the primary MSA is envisaged to be the Artificial Intelligence Development and Safety Commission (KRiBSI), although, depending on the sector concerned, other competent authorities may also be involved. In Poland, FRABs include, inter alia, the Personal Data Protection Office (UODO), the Patient Rights Ombudsman, the National Labour Inspectorate, and the Children's Rights Ombudsman. Pursuant to Regulation (EU) 2024/1689, the list of such bodies is subject to ongoing updates.

In principle, this amendment should be assessed positively; however, it is subject to certain reservations.

a) Positive Aspects

The designation of the MSA as a centralised point of contact may bring a number of benefits, including improved coordination between authorities and the establishment of a standardised procedural framework (notably, a single point of contact instead of multiple bodies). The proposed obligation of close cooperation and mutual assistance (new Article 77(1b)) may further enhance information exchange, particularly in cross-border cases.

It should also be positively assessed that the proposal removes the limitation of Article 77(1) AIA exclusively to high-risk systems listed in Annex III. This amendment naturally broadens the potential scope of fundamental rights protection.

b) Role of the MSA in the Handling of Requests

The proposed amendment does not define with sufficient precision the role of the MSA in handling requests submitted by FRABs. In our assessment, the role of the MSA should be limited to organisational and coordinating functions – such as receiving the request, ensuring a communication channel with the provider or deployer, and verifying formal requirements – thus acting as a procedural "hub." The substantive assessment of the request, including the evaluation of its merits, should remain within the competence of

FRABs. This allocation of responsibilities should be explicitly clarified in the proposed amendment to Article 77(1) AIA.

Absent such clarification, there is a risk that MSA mediation could function as a filtering or blocking mechanism, potentially weakening the effectiveness of FRABs and, consequently, the overall protection of fundamental rights.

c) Risk of Limiting the Scope of Information Transmitted

The proposed Article 77(1a) AIA also significantly alters the scope of FRABs' powers by shifting from the ability to request documentation "created or maintained under this Regulation" (i.e., documentation prepared or kept by the operator pursuant to Article 77(1) AIA) to documentation "created or maintained from the relevant market surveillance authority." It further provides that the MSA shall request information from the operator "where necessary," which may in practice leave the MSA with discretionary authority to assess whether such a request is required. As the Digital Omnibus on AI proposal does not provide FRABs with the possibility of independently addressing the operator, there is a risk that the scope of information received by FRABs may be indirectly shaped by the MSA.

d) Risk of Inefficiency and Delays

In their joint Opinion 1/2026, the EDPB and EDPS observe that requiring FRABs to obtain information exclusively through the MSA may, in practice, lead to inefficiencies and delays in their actions. The introduction of an additional intermediary in the procedure may prolong the response time in situations involving potential violations of fundamental rights.
The EDPB and EDPS therefore recommend that the Regulation explicitly provide that market surveillance authorities are obliged to transmit information requested by FRABs without undue delay, both at national level and in cross-border cases.

2.2.5. Proposal to Introduce Article 4a AIA – Changes to the Scope of Processing of Special Categories of Personal Data

Under Article 10(5) AIA, providers of high-risk AI systems may, on an exceptional basis, process special categories of personal data where this is strictly necessary for the purposes of detecting and correcting bias in such systems, in accordance with Article 10(2)(f) and (g) AIA. Such processing is subject to the condition that appropriate safeguards for the fundamental rights and freedoms of natural persons are applied.

The Digital Omnibus on AI proposal introduces a new provision, Article 4a, which would replace Article 10(5) AIA and, importantly, significantly broaden both the categories of entities concerned and the activities covered.

a) Entities and Activities Covered

The proposal extends the mechanism permitting the processing of special categories of personal data for the purpose of detecting and correcting bias not only to providers, but also to deployers. Furthermore, pursuant to Article 4a(2), the mechanism would apply not only to high-risk AI systems but also to a broader range of AI systems and models, including general-purpose AI (GPAI) models. This substantially increases both the number of entities and the variety of contexts in which the processing of sensitive data would be permissible.

The extension of the circle of authorised entities raises concerns. Deployers, unlike providers, often do not have full knowledge of the architecture of the AI system or access to information regarding the data used during the training phase. This may hinder a reliable assessment of whether the processing of special categories of personal data is genuinely necessary for the purposes of detecting and correcting bias.

b) Standard of Necessity and the Position of the EDPB and EDPS

Article 10(5) AIA currently requires that the processing of special categories of personal data be "strictly necessary." The Digital Omnibus on AI proposal lowers this threshold: Article 4a(1) refers to processing that is "necessary," while Article 4a(2) introduces the criterion of "necessary and proportionate." The softening of the necessity requirement raises concerns in light of the restrictive approach under EU law to the processing of special categories of personal data. Pursuant to Article 9(1) GDPR, such processing is, as a rule, prohibited, and exceptions must be interpreted narrowly.

In their joint Opinion 1/2026, the EDPB and EDPS underline that although combating bias constitutes a legitimate and important objective, the Commission's proposal weakens the protection standard by replacing the requirement of "strict necessity" with ordinary "necessity." The bodies further recommend that, in order to limit the risk of abuse, the situations in which providers and deployers may rely on the exception laid down in Article 4a – particularly in relation to AI systems and models other than high-risk systems – should be clearly defined and restricted to cases where the risk of significant negative effects resulting from bias is genuinely serious.

c) Risk of Normalisation of Mass Data Collection

The introduction of Article 4a in the proposed wording may contribute to the normalisation of the processing – and in practice also the acquisition and aggregation – of special categories of personal data under the broadly formulated objective of "bias detection and correction." Extending this exception to all AI systems and models (and not only high-risk systems), as well as to a wide range of entities including deployers, increases the risk that processing sensitive data may become a default or precautionary ("just in case") practice. This concern is reinforced by the fact that the assessment of whether such processing is genuinely necessary would, in practice, be left to numerous individual entities, which complicates the establishment of uniform standards and the effective verification of the proportionality of such actions.

In this context, the Irish Human Rights and Equality Commission (IHREC) has pointed to the risk that the proposed Article 4a may broaden access to sensitive data in a manner that facilitates their mass collection and potentially enables profiling and surveillance practices under the pretext of "bias detection," without sufficiently robust enforcement mechanisms. As a result, a mechanism intended to limit discrimination may paradoxically increase the scale of operations involving particularly sensitive data and hinder effective control over their scope and purpose (see Letter to Department of Enterprise, Tourism and Employment on EU Interpretative Note Art 77 bodies and Digital Omnibus, 8.12.2025).

d) Critical Assessment

From the perspective of fundamental rights protection, the proposed amendments give rise to justified concerns. Special categories of personal data — such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health data, or sexual orientation — are subject to enhanced protection precisely because of the discriminatory potential inherent in their processing.

Extending the possibility of processing such data to a broader range of AI systems and entities, while simultaneously lowering the standard from "strict necessity" to ordinary "necessity," creates a risk that an exception introduced for the purpose of combating discrimination may be applied in a manner contrary to that objective.

V. Summary and Conclusions

The Digital Omnibus and the Digital Omnibus on AI package, despite their declared objective of simplification and strengthening European competitiveness, contain proposals that give rise to serious concerns from the perspective of fundamental rights protection and the coherence of the EU legal order.

Of particular concern are the proposed amendments to the GDPR which, under the guise of "technical clarification," may in practice result in a substantive lowering of the level of personal data protection guaranteed under EU law.

In the assessment of the of the experts of the New Technologies Committee of the National Bar Council of Attorneys-at-Law, consideration should be given to the following:

1) Abandoning the proposed amendments to the definition of personal data in Article 4(1) GDPR, which introduce a subjective element into what has thus far been an objective concept and thereby distort the logic of Recital 26.

2) Withdrawing the proposal to introduce Article 88c GDPR, as it would undermine the principle of technological neutrality, conflict with the CJEU case-law, and appear redundant in light of the existing interpretation adopted by the EDPB (Opinion 28/2024).

3) Withdrawing the proposed Article 9(2)(k) GDPR and maintaining the regulation of processing of special categories of personal data for the purposes of bias detection within Article 10(5) AIA, while preserving the "strict necessity" standard.

4) Maintaining the prohibitory character of Article 22 GDPR, including the requirement of "necessity" under Article 22(2)(a) GDPR, as a fundamental safeguard protecting individuals against automated decision-making.

5) Abandoning the proposed extension of exemptions from information obligations under Article 13 GDPR, beyond the already existing limitation set out in Article 13(4).

6) Focusing efforts on strengthening the enforcement of the existing GDPR framework and on issuing interpretative guidance by the EDPB, rather than amending the substantive provisions of the Regulation.

7) Conducting a comprehensive fundamental rights impact assessment prior to the adoption of the proposed amendments, both with regard to the Digital Omnibus and the Digital Omnibus on AI.

8) With respect to the proposed amendments to Articles 111 and 113 AIA (application schedule): replacing the "moving deadline" mechanism (Article 113 AIA) with a fixed date of application in order to eliminate legal uncertainty or alternatively, should the flexible mechanism be retained, specifying a clear deadline within which the Commission must adopt its decision, thereby ensuring that obligated entities benefit from a minimum guaranteed implementation period. Consideration should also be given to differentiating the deferral according to categories of obligations. In particular, requirements whose application does not depend on the availability of detailed technical standards (such as transparency and information obligations) could enter into force in accordance with the original timetable.

9) Maintaining the mandatory character of provisions concerning AI literacy (Article 4 AIA), in line with the recommendation of the EDPB and EDPS. Rather than abolishing the existing obligation, consideration should be given to issuing practical guidance for providers and deployers on the implementation of AI literacy requirements.

10) Amending the proposed Article 77(1a) AIA to introduce an explicit obligation for the market surveillance authority (MSA) to act "without undue delay," both in national and cross-border cases, and clarifying that the substantive assessment of the merits of a request should remain within the competence of FRABs.

11) Maintaining the obligation to register in the EU database AI systems that a provider has classified as not constituting high-risk systems.

12) Retaining the current wording of Article 10(5) AIA and refraining from introducing Article 4a, which would extend the scope of processing of special categories of personal data. Alternatively, should Article 4a be maintained, its application should remain limited to high-risk systems, with restoration of the "strictly necessary" standard. Any extension beyond the category of high-risk systems should be permitted exclusively in strictly defined cases involving a

serious risk of bias, accompanied by enhanced documentation and supervisory safeguards.

13) Ensuring broader and more balanced consultations in the course of further legislative work, including meaningful participation of civil society organisations, academic experts, fundamental rights protection bodies, and professional self-governments.

***

Genuine simplification does not consist in rewriting existing legislation, but in ensuring the clear and consistent enforcement of the rules already in force, accompanied by robust supervision. Europe's credibility as a defender of digital rights depends on preserving the level of protection it has developed, rather than weakening it under deregulatory pressure.

We hope that the above remarks will be duly taken into account in the further legislative process.

NATIONAL COUNCIL
OF ATTORNEYS-AT-LAW

Warsaw, February 2026