BEYOND SIMPLIFICATION

HOW THE DIGITAL OMNIBUS WEAKENS CORE GDPR SAFEGUARDS

EXECUTIVE SUMMARY [1]

The Digital Omnibus is presented as a technical simplification exercise. However, in the area of data protection, it introduces substantive changes that go well beyond procedural streamlining. The proposal affects core elements of the General Data Protection Regulation (GDPR), including its scope, lawful bases for processing, protections for sensitive data, and key safeguards against abuse. **Several of these changes would lower the level of protection for personal data and weaken mechanisms that are central to effective enforcement, and reduce legal certainty for individuals and collectives, controllers, and Supervisory Authorities (SAs) alike.** A further concern lies in the **cumulative interaction of the proposed amendments**. Considered together (and also with those put forward in the AI Omnibus proposal), they weaken the practical force of purpose limitation by making it easier to reframe data reuse as AI development or scientific research, while simultaneously reducing transparency and access obligations and, in some cases, narrowing the scope of the GDPR itself.

While the shortcomings of the proposal affect all amendments, the level of concern they raise is not uniform. **The proposed changes differ significantly in their nature and impact.** This document therefore examines them from the most to the least concerning, based on their structural effects on the GDPR. **Some proposals should not be pursued at all, as they would undermine core elements of the Regulation. Others amount to substantive policy choices that, if considered, require a full legislative proposal and a proper democratic debate**, in line with the Better Regulation Guidelines and within the

1 This part of the paper focuses exclusively on the GDPR components of the Digital Omnibus. It accompanies a separate position paper on ePrivacy, reflecting the importance of keeping both frameworks distinct, coherent, and complementary. The GDPR and ePrivacy protect different fundamental rights and rely on different safeguards. Addressing them together through horizontal simplification risks weakening both.

framework of the Digital Fitness Check. They cannot be introduced through a horizontal simplification package. Finally, a limited number of proposals could be considered acceptable as genuinely targeted amendments, provided they are significantly tightened and carefully framed.

The proposal is presented as a simplification measure intended to support small and medium-sized enterprises. However, **many of the amendments examined in this paper do not primarily address administrative burdens faced by smaller organisations**. Instead, they are **far more likely to benefit actors operating extensive data infrastructures than smaller organisations seeking legal clarity and practical guidance**. That is because they reshape core substantive safeguards, particularly in areas such as AI development, data reuse, and large-scale processing.

The most significant GDPR changes analysed in this part of the paper include:

Definition of personal data and scope of the GDPR (Articles 4 and 41)

- The proposal alters how identifiability is assessed and allows certain pseudonymised data to fall outside the GDPR for specific actors. **This would undermine legal certainty and fragment the application of EU data protection law at the very first step.**

- Changes to the definition of personal data **affect whether the GDPR applies at all** and should not be pursued under any circumstances.

AI-related processing and the reframing of legitimate interest (Article 88c)

- The introduction of a dedicated provision for AI training and operation links large-scale model development to legitimate interest. While legitimate interest can be an acceptable legal basis when the three-step test is correctly applied, **this provision could be read as creating a presumption of legality for extensive data reuse**.

- In practice, this approach would **risk weakening purpose limitation, marginalising consent, and rendering the right to object ineffective**. It also **undermines the GDPR's principle of technological neutrality**. Any such shift would constitute a substantive change to the Regulation and, if considered at all, would require a full legislative process.

Special category data and biometric data (Articles 9(2)(k) and 9(2)(l))

- New derogations allow sensitive data to remain in AI systems where removal is considered disproportionate and permit broader use of biometric authentication **under vague conditions**.

- In practice, **these changes would weaken protections for both explicit and inferred sensitive data**, particularly in large-scale and opaque systems, while reducing legal certainty.

Expansion of scientific research exemptions and weakening of purpose limitation (Articles 4 and 5)

- The proposal expands the definition of 'scientific research', blurring the boundary between genuine public-interest research and commercial data exploitation. **This risks allowing large-scale commercial activities, including AI development and optimisation, to rely on research-related derogations designed for scientific and public-interest purposes.**

- The amendment to Article 5(1)(b) weakens the principle of purpose limitation by declaring further processing for research purposes compatible with the original purpose independently of the compatibility assessment in Article 6(4). **In combination with the broader definition of research, this significantly expands the scope for repurposing personal data with reduced safeguards and oversight.**

Automated decision-making (Article 22)

- The proposal s**hifts the provision from a prohibition with limited exceptions to a permission with conditions**, weakening its role as a structural safeguard.

- The proposal **also alters the necessity test by allowing automated decision-making to be considered necessary for entering into or performing a contract** even where the same decision could be taken by non-automated means, significantly expanding controllers' discretion.

- In practice, **automated decision-making could become the default** in areas such as employment, credit, and access to services, while human intervention risks being reduced to a formal rather than meaningful safeguard.

Right of access (Article 12(5))

- The proposal allows controllers to refuse, delay, or charge for access requests based on claims of abuse, excessiveness, presumed prior knowledge, or on the ground that a request is not exclusively related to data protection purposes. **This would weaken a central tool for uncovering unlawful processing, discrimination, and profiling, and reduce the effectiveness of both individual and collective oversight.**

Right to information (Article 13)

- Expanded exemptions allow generic, delayed, or withheld information, particularly in research and AI contexts. This could **significantly reduce transparency precisely where risks are highest, making it harder for people to understand how and why their data is used**.

Personal data breach notification (Article 33)

- Higher notification thresholds and procedural changes could **reduce reporting to SAs and affected individuals**, limiting early detection of systemic problems and weakening independent oversight.

Data Protection Impact Assessments (DPIAs) (Article 35)

- Even where the objective of harmonisation is legitimate, care is needed to ensure that expanded exemptions and increased reliance on whitelists do not weaken preventive safeguards, reduce the role of prior consultation with SAs, or shift risk assessment disproportionately towards internal, controller-led processes.

Taken together, both individually and cumulatively, these changes **would shift the GDPR away from a preventive, rights-based framework towards one that relies more heavily on discretion, self-assessment, and downstream risk management**. This risks **reinforcing the structural power imbalance between controllers and individuals** and **weakening the mechanisms that allow people to effectively exercise their right** to the protection of personal data under Article 8 of the Charter of Fundamental Rights of the European Union.

Any legislative changes that reduce these safeguards must therefore be assessed in light of Article 52(1) of the Charter, which requires that limitations on fundamental rights respect their essence and comply with the principles of necessity and proportionality.

SIMPLIFICATION AND DEREGULATION ARE NOT THE SAME

The stated objective of the Digital Omnibus is simplification. In the area of data protection, most proposed amendments go beyond simplifying procedures or reducing administrative burden. Some, in fact, will further complicate compliance and enforcement. **They moreover alter substantive rules and undermine people's rights.** Simplification could support compliance and enforcement. It can clarify obligations, harmonise procedures, improve cooperation between authorities, or reduce unnecessary duplication. It does not require redefining core legal concepts or expanding derogations from fundamental safeguards.

This distinction matters. **Changes to substantive data protection rules affect how rights under Articles 7 and 8 of the Charter operate in practice. They also affect the coherence of the wider EU digital rulebook**, including instruments that rely on the GDPR as a baseline for risk assessment, accountability, and enforcement.

For this reason, procedural simplification and substantive policy choices must be clearly separated. A majority of amendments examined in this paper amount to policy choices about the acceptable level of data reuse, automation, and discretion afforded to controllers. **If considered at all, such choices require a full legislative proposal, supported by a proper fundamental rights impact assessment and debated transparently in the context of the Digital Fitness Check**.

Other proposals go further. First and foremost, **changes affecting the definition of personal data and the material scope of the GDPR raise structural concerns that cannot be addressed through any revision exercise**. These concepts determine whether the GDPR applies in the first place. Reopening them would undermine legal certainty and weaken protection at its foundation.

A further concern lies in the **cumulative interaction of the proposed amendments**. Considered separately, the changes affect lawful bases, transparency, research derogations, access rights, and the scope of the GDPR. Considered together, however, they also weaken the practical force of purpose limitation. Data initially collected in one context could more easily be repurposed for AI development or reframed as scientific research, while the corresponding duties to inform individuals or provide access are reduced. In some cases, the same proposal also seeks to narrow the conditions under which such data remain subject to the GDPR at all.

The result is not only greater flexibility for controllers. It is a structural shift away from the principle that personal data should not be reused for new purposes without clear legal justification, transparency, and effective safeguards. **Taken together, these changes risk creating situations where personal data are reused extensively while**

individuals receive little or no information about such processing, significantly weakening the practical ability to detect, contest, or remedy unlawful data use.

The sections that follow reflect the distinction between those changes that affect the applicability of the GDPR itself and those that weaken safeguards within an otherwise intact framework.

SECTION 1.

DEFINITION OF PERSONAL DATA AND SCOPE OF THE GDPR

(Articles 4 and 41 and related recitals)

Why these changes are the most serious and should not be pursued

The most far-reaching amendments in the Digital Omnibus concern the definition of personal data and the material scope of the GDPR. **These provisions determine whether the Regulation applies at all. Every other right, safeguard, and enforcement mechanism depends on this threshold.**

For this reason, changes to Articles 4 and 41 raise concerns of a different nature and magnitude than any other amendment in the package. They do not merely weaken specific obligations or introduce new flexibilities. They **alter the entry point of EU data protection law**, redistribute regulatory discretion, and directly affect legal certainty across the Union.

Unlike other proposals examined in this paper, these changes cannot be framed as policy trade-offs or matters of legislative balance. They **go to the constitutional core of EU data protection law**. For that reason, they should not be pursued through a simplification package, nor revisited in any future legislative exercise, including a Digital Fitness Check.

From an objective assessment of identifiability to a controller-centric approach

Article 4(1) GDPR currently defines personal data broadly, covering any information relating to an identified or identifiable natural person. Recital 26 clarifies that identifiability must be assessed objectively and contextually, taking into account all means reasonably likely to be used, directly or indirectly, in the real world.

This approach ensures a single, EU-wide standard. Whether data qualify as personal data does not depend on what a specific controller claims to be able to do, but on whether identification is realistically possible within the broader processing environment.

The Digital Omnibus alters this logic. By placing greater emphasis on what a specific controller considers 'reasonably likely', the proposal would make the qualification of the same dataset depend on who holds it, rather than on its objective characteristics and on the wider data ecosystem.

In practice, this would allow identical data to be treated as personal data by some actors and as non-personal data by others, even where re-identification risks clearly persist elsewhere in the processing chain. **This would fragment the application of the GDPR, undermine equal protection, and erode legal certainty for individuals, controllers, and SAs alike.**

Article 41, pseudonymised data, and the expansion of Commission discretion

The proposal goes further by introducing a new Article 41, which empowers the Commission to determine, through implementing acts, that certain pseudonymised data no longer qualify as personal data for specific entities or contexts.

Under the current GDPR, pseudonymised data remain personal data because re-identification remains possible, whether by the same actor or by others with access to additional information. This reflects a risk-based and ecosystem-aware approach, in which safeguards apply precisely because risks do not disappear simply because identifiers are replaced.

Article 41 departs from this logic in two ways. First, **it creates a legal pathway for large datasets, identifiers, or behavioural logs to fall outside the GDPR even where identification risks persist downstream**. Once such data are treated as non-personal for certain actors, the GDPR ceases to apply at the very stage where aggregation, reuse, and combination generate the highest risks.

Second, it **reallocates core determinations about the scope of fundamental rights protection to the Commission through implementing acts**. This shifts decisions that currently follow from directly applicable law and judicial interpretation into a discretionary, executive-driven process. Such a move undermines legal certainty and predictability, both of which are essential for fundamental rights protection and for the uniform application of EU law.

Selective codification of case law

In support of this shift, reference is made to recent case law, in particular the judgment of the Court of Justice of the European Union in the SRB case. That judgment concerned a highly specific factual and institutional context, in which access to the data was strictly limited and the assessment of identifiability was tied to concrete safeguards and conditions. Crucially, the Court's reasoning remained contextual and risk-based. It did not establish a general rule allowing pseudonymised data to fall outside the scope of the GDPR whenever a particular controller claims not to have the means to identify individuals.

The Digital Omnibus goes beyond what the Court assessed. By codifying a narrow reading of identifiability detached from its factual context, the proposal transforms a case-specific assessment into a general regulatory mechanism. In doing so, it abstracts from the safeguards and access limitations that were central to the Court's reasoning and repurposes the judgment to justify a broad exclusion of certain pseudonymised data from the GDPR. **This selective codification does not clarify the law. It alters it, while weakening the legal certainty that the GDPR was designed to provide.**

Systemic consequences across the digital rulebook

Weakening the definition of personal data does not remain confined to the GDPR. **Lowering the threshold of applicability would affect the operation of the entire EU digital rulebook**, including instruments that rely on the GDPR as a baseline for risk assessment, accountability, and rights protection.

If data fall outside the GDPR at the definition stage, downstream safeguards become irrelevant. Transparency obligations, access rights, restrictions on automated decision-making, and supervisory oversight no longer apply. No amount of guidance or enforcement can compensate for a narrowed scope of application.

Lowering the threshold for what qualifies as personal data would also create **procedural obstacles for individuals seeking to enforce their rights**. In many situations, individuals would first need to demonstrate that the information in question qualifies as personal data in order to trigger the GDPR. Yet without access to the relevant data or processing context, this becomes extremely difficult in practice. The result is a circular situation in which individuals must prove the applicability of the Regulation without access to the information necessary to do so, thereby weakening the effectiveness of remedies and oversight.

This shift would also have **consequences for tracking technologies widely used in online services**. Many advertising and analytics systems rely on identifiers such as cookies, device identifiers, or hashed identifiers that allow individuals to be singled out across services or over time. If such identifiers are no longer consistently treated as personal data and instead depend on the controller's perspective, large parts of the tracking ecosystem could fall outside the GDPR despite enabling persistent monitoring and profiling.

SECTION 2.

AI-RELATED PROCESSING AND THE REFRAMING OF LEGITIMATE INTEREST

(Article 88c and related recitals)

Why this is a structural policy choice, not a simplification measure

Article 88c introduces a dedicated provision addressing the use of personal data for the development, training, and operation of artificial intelligence systems. It does so by explicitly linking such processing to legitimate interest under Article 6(1)(f) GDPR.

This is not a clarification. **It amounts to a substantive policy choice about the acceptable conditions for large-scale data reuse in the context of AI**. As such, it cannot be introduced through a horizontal simplification package. If considered at all, it would require a full legislative proposal, supported by a fundamental rights impact assessment, and debated in the context of the Digital Fitness Check.

More fundamentally, **the introduction of a technology-specific lawful basis risks undermining one of the GDPR's core design principles, namely its technological neutrality**. The GDPR deliberately regulates processing operations and risks, rather than specific technologies, in order to remain future-proof and consistently applicable across sectors and technical developments. Singling out AI systems for bespoke treatment departs from this approach, creates pressure for further technology-specific carve-outs, and weakens the coherence and legal certainty of the framework as a whole.

From contextual balancing to structural permission

Under the GDPR, legitimate interest is a lawful basis like any other, provided it is applied contextually and subject to a strict case-by-case assessment. This requires a rigorous

three-step test, including necessity and balancing, and full consideration of the data subject's fundamental rights and reasonable expectations. **The December 2024 EDPB Opinion on AI training already clarified how these requirements apply in the context of AI systems, confirming that existing GDPR rules are sufficient when properly enforced.**

Article 88c alters how this lawful basis operates in practice. **By introducing a specific provision for AI-related processing, the proposal could elevate certain forms of large-scale data reuse from a contextual assessment to a structurally recognised category of lawful processing.**

Even if the formal elements of the legitimate interest test remain unchanged, the existence of a dedicated article creates a strong interpretative signal. In practice, **it could be read as a presumption that AI training and operation are, by default, compatible with the legitimate interests of controllers.**

In practice, the development and operation of AI systems frequently relies on very large and heterogeneous datasets that may combine data collected directly from users, obtained from third parties, or scraped from publicly accessible sources. Article 88c does not meaningfully limit the scale or origin of such data. As a result, **the provision could enable extensive reuse of personal data across contexts while relying on a lawful basis that was originally designed for more limited and contextual forms of processing.**

Erosion of the right to object in practice

Under Article 21 GDPR, the right to object is meant to function as a meaningful counterweight when processing is based on legitimate interest. Controllers must demonstrate compelling legitimate grounds that override the interests, rights, and freedoms of the data subject.

Article 88c risks emptying this safeguard of its practical effect. Where AI training and operation are framed as structurally legitimate and socially expected forms of processing, objections become extremely difficult to sustain in practice. **Individuals are placed in a position where they must object to processing that is large-scale, continuous, and diffuse, often without knowing whether their data are included, how they are used, or how objection could meaningfully be implemented.**

In such contexts, controllers can plausibly argue that individual objections cannot be accommodated without undermining the system as a whole. **As a result, the right to object risks becoming largely theoretical, preserved in form but ineffective in substance.** This is a qualitative shift. It transforms the right to object from an enforceable safeguard into an abstract possibility that is structurally discouraged.

Impact on legal certainty and enforceability

The introduction of Article 88c would also erode legal certainty. By reframing AI development as a typical and anticipated form of processing under legitimate interest, the proposal blurs the boundaries between exceptional reuse and routine processing. **Controllers, data subjects, and SAs would face increased uncertainty as to when consent is required, when objection must be upheld, and how necessity and balancing should be assessed in practice.**

This uncertainty is not incidental. It flows directly from the attempt to normalise an activity that is inherently broad, evolving, and difficult to delimit through a general lawful basis. As a result, enforcement risks becoming more fragmented and reactive, with key determinations deferred to ex post assessments rather than constrained ex ante by clear legal limits.

Interaction with other safeguards and cumulative effects

Article 88c cannot be assessed in isolation. Its effects compound when read together with other proposed amendments, including expanded research exemptions, new derogations for special category data, and weaker transparency and access rights.

Taken together, these changes could allow extensive AI training and model operation to rely on layered justifications that are difficult to contest in practice. The cumulative effect would be to reduce the practical relevance of individual rights, including objection and erasure, and to shift risk management further towards internal, controller-led processes.

This dynamic also affects the coherence of the wider EU digital rulebook. Instruments that rely on the GDPR as a baseline for accountability and risk mitigation assume that lawful bases remain constrained, contestable, and enforceable. Weakening those constraints at the GDPR level has consequences well beyond this Regulation.

SECTION 3.

SPECIAL CATEGORY DATA AND BIOMETRIC

(Articles 9(2)(k), 9(2)(l), and related changes)

Why narrowly framed derogations create systemic risks

The Digital Omnibus introduces new derogations to the protection of special category data under Articles 9(2)(k) and 9(2)(l), alongside a significant expansion of the scientific research framework. **On their face, these changes might appear targeted and limited. In practice, they interact with other amendments in ways that substantially weaken protection for sensitive and inferred data.**

These provisions cannot be assessed in isolation. Their effects depend on how they operate together with the proposed inclusion of Article 88c, the proposed changes to the AI Act, and weaker transparency, access, and objection rights. When read as a package, t**hey create structural pathways for sensitive data to remain embedded in large-scale processing and AI systems, while reducing the ability to detect, contest, or remove such data.**

Article 9(2)(k): sensitive data, AI systems, and the normalisation of retention

Article 9(2)(k) allows special category data to remain in AI training or operation where removing such data would require disproportionate effort. This marks a significant shift in the logic of sensitive data protection.

Under the GDPR, the processing of special category data is prohibited as a rule, with narrowly defined exceptions. The focus is on whether such data should be processed at all. **Article 9(2)(k) reverses this approach by accepting the presence of sensitive data within AI systems and shifting the question to whether their removal is feasible.**

This shift is particularly problematic when read together with the proposed amendment to Article 4 of the AI Act, which allows the processing of special category data for the purpose of detecting, monitoring, and correcting bias in AI systems. Framed as a safeguard, this provision creates a justification for collecting or inferring sensitive attributes in order to assess fairness.

In combination, these provisions normalise the presence of sensitive data inside AI systems. Controllers can argue that sensitive attributes are needed to measure bias and that, once embedded in training data or models, removing them would require disproportionate effort. The result is a strong incentive to retain sensitive and inferred

data as a functional necessity rather than treating them as an exceptional category requiring heightened protection.

This risk is **particularly pronounced in behavioural profiling systems, where sensitive attributes are often inferred from patterns of online activity, browsing behaviour, or location data rather than collected directly**. Once such attributes are embedded in large datasets or models, identifying and removing them becomes technically and legally difficult.

This interaction weakens the practical operation of key rights under the GDPR, including the right to erasure and the right to object. **Once sensitive data are treated as structurally embedded, individual rights become extremely difficult to exercise in practice, even if they remain formally intact.**

The reliance on 'disproportionate effort' further erodes legal certainty. Individuals cannot reasonably predict when their sensitive data will be protected or retained, and SAs are left to assess complex technical claims without clear legal benchmarks. Rather than reinforcing safeguards, Article 9(2)(k), especially when combined with the AI Act's bias-related provisions, shifts the GDPR towards tolerance of sensitive data retention in the name of system optimisation.

Article 9(2)(l): biometric data, verification means, and the fiction of 'sole control'

Article 9(2)(l) introduces a new derogation for biometric data used for authentication where the biometric data or the verification means are under the 'sole control' of the data subject. This formulation is critical. **By allowing reliance on control over either the biometric data or the verification process, the provision lowers the threshold of protection and fragments the notion of control.** It does not require that individuals exercise effective control over the biometric system as a whole.

In most real-world deployments, biometric authentication relies on a combination of hardware, software, and verification mechanisms controlled or designed by manufacturers, platform providers, or service operators. Even where biometric templates are stored locally, verification parameters, updates, error thresholds, or fallback mechanisms typically remain outside the individual's control. While authentication systems may serve legitimate purposes in limited contexts, **biometric identifiers are inherently sensitive and difficult to revoke once compromised**. Expanding the circumstances in which biometric verification can be used risks normalising infrastructures that rely on the routine processing of biometric identifiers across services and environments. Without strict necessity tests and clear safeguards, this could contribute to the gradual expansion of biometric monitoring practices.

The disjunctive wording ('data or the verification means') allows controllers to claim compliance while retaining decisive influence over critical elements of the system. **This creates a legal fiction of 'sole control' that does not reflect how biometric systems operate in practice.**

As a result, **Article 9(2)(l) undermines legal certainty and weakens the protection traditionally afforded to biometric data under Article 9**. Over time, it risks enabling broader biometric use with reduced safeguards, particularly when combined with weakened transparency, access, and objection rights.

Cumulative effects on rights, enforceability, and legal certainty

Taken together, Articles 9(2)(k), 9(2)(l), and the expanded research framework (below) weaken the protection of special category data precisely in contexts where risks are highest. They normalise the presence of sensitive and biometric data in large-scale systems while reducing the effectiveness of rights designed to limit such processing.

These changes would **further erode legal certainty by making the scope of protection dependent on vague standards, technical feasibility, and internal assessments rather than clear legal limits**. As with Article 88c, the result is a shift away from preventive protection towards after-the-fact risk management, with enforcement becoming more difficult and fragmented.

Why these changes require (if at all) a full legislative process

While these provisions do not redefine the scope of the GDPR *per se*, they recalibrate its internal balance in a way that **directly affects fundamental rights, including the protection of sensitive data and the effective exercise of individual rights**.

Such recalibration cannot be justified as simplification. If considered at all, these changes require a full legislative proposal, grounded in a clear policy debate and accompanied by a proper assessment of impacts on rights, legal certainty, and enforcement. They should not be introduced through the Digital Omnibus.

SECTION 4.

EXPANSION OF SCIENTIFIC RESEARCH EXEMPTION (Article 4 definition, Article 5 purpose limitation and related derogations)

The proposal does not merely clarify the treatment of research-related processing. It expands both the range of activities that may qualify as scientific research and the conditions under which personal data collected for one purpose may subsequently be reused for those activities. By broadening the definition of research and weakening safeguards governing further processing, the proposal significantly increases the scope for large-scale reuse of personal data under the research framework.

Broadening the definition of scientific research

The proposal expands the definition of 'scientific research' in Article 4. While **the GDPR has always recognised the importance of research activities, the existing framework relies on a contextual and purpose-based understanding of research.** It does not treat all data-driven innovation as research, nor does it grant blanket exemptions to large-scale commercial data processing. **While research exemptions serve an important societal purpose, the proposed changes blur the boundary between public-interest research and commercial data exploitation.**

By broadening the notion of scientific research and relaxing transparency and reuse constraints, **the proposal could allow commercial AI development, testing, and optimisation to benefit from safeguards designed for genuinely research-driven activities.** In such contexts, individuals may receive only generic information or none at all, and data collected for one purpose can be reused extensively for another.

The expansion of research-related derogations also interacts with existing exemptions from transparency obligations (see below), particularly where personal data are obtained indirectly. Under the GDPR, controllers may refrain from informing individuals where providing such information would involve disproportionate effort, including in research contexts. If the notion of scientific research is broadened while this exemption remains available, individuals may never be informed that their data are being used in large-scale research or AI training activities.

Without clearer boundaries, commercial actors engaged in data-intensive product development may rely on research-related derogations to justify extensive data reuse while limiting transparency towards individuals. Clarifying the definition of research is therefore not just a technical adjustment: it directly affects the scope of multiple GDPR

safeguards and requires careful consideration through a full legislative process rather than a simplification package.

Weakening the principle of purpose limitation (Article 5(1)(b))

The proposal also modifies the way the GDPR treats further processing of personal data for archiving in the public interest, scientific or historical research, and statistical purposes. The amendment to Article 5(1)(b) strengthens the presumption that such processing is compatible with the original purpose of collection and removes an important safeguard that currently governs the repurposing of personal data.

Under the current wording of the GDPR, **personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a manner incompatible with those purposes**. Article 5(1)(b) clarifies that further processing for archiving in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1), is not considered incompatible with the initial purpose.

This formulation reflects a balanced approach. It recognises the societal value of research activities while ensuring that the principle of purpose limitation remains meaningful. **Controllers relying on research-related processing must still comply with the broader framework of the GDPR.** They must rely on a lawful basis under Article 6, respect the safeguards required under Article 89(1), and, where relevant, assess compatibility under Article 6(4).

Article 6(4) provides the structured compatibility test used to determine whether further processing remains compatible with the purpose for which personal data were originally collected. This assessment requires controllers to consider several factors, including the link between the original and new purposes, the context in which the data were collected, the nature of the personal data, the possible consequences for individuals, and the existence of safeguards such as pseudonymisation.

The proposed amendment introduces two important changes.

1. First, the wording would shift from stating that research-related processing is "not considered to be incompatible" with the initial purpose to stating that it is "considered to be compatible with the initial purposes." This change strengthens the presumption of compatibility and moves the provision closer to an automatic rule allowing reuse of personal data for research purposes.

2. Second, and more significantly, the amendment specifies that this compatibility applies independently of the conditions set out in Article 6(4). This effectively

removes the compatibility test that currently governs further processing of personal data.

By excluding the Article 6(4) assessment, the proposal removes an important accountability mechanism. Controllers invoking research, statistical or archiving purposes would no longer be required to examine whether the new processing purpose remains compatible with the original context of collection.

This change must also be understood in the broader context of large-scale data processing and artificial intelligence development. Research-related purposes are increasingly invoked in activities such as data analytics, algorithmic development and AI training. Presuming compatibility without requiring a structured compatibility assessment lowers the threshold for repurposing personal data across different contexts.

Taken together with the proposed expansion of the definition of scientific research, the amendment to Article 5(1)(b) risks significantly broadening the scope for data reuse under the research framework. Personal data collected in one context may be repurposed for large-scale research or AI development activities with fewer safeguards and reduced oversight.

Why these changes should be rejected

The proposed expansion of the definition of scientific research and the amendment to Article 5(1)(b) should be rejected because, taken together, they **significantly broaden the scope for reusing personal data while weakening safeguards that currently limit such reuse**.

First, the proposed definition risks blurring the distinction between public-interest research and commercial data exploitation. The current GDPR framework allows flexibility in the interpretation of research while preserving safeguards designed to prevent large-scale commercial data processing from benefiting from research-related derogations. **Broadening the definition without clear limits could allow commercial actors engaged in data-intensive innovation to rely on exemptions originally designed for genuine scientific research**.

Second, the amendment to Article 5(1)(b) removes an important accountability mechanism that currently governs the repurposing of personal data. By declaring further processing for research purposes compatible with the initial purpose independently of the compatibility assessment in Article 6(4), the proposal **eliminates the structured test that currently ensures that secondary uses of personal data remain proportionate and contextually justified.**

Third, the interaction between these changes risks creating a framework in which personal data collected for one purpose may be reused for a wide range of research or innovation activities with reduced safeguards. **In combination with existing transparency exemptions, individuals may receive little or no information about how their personal data are reused in large-scale research or artificial intelligence development activities**.

Finally, **the existing GDPR framework already provides mechanisms that enable research activities while preserving the principle of purpose limitation and ensuring appropriate safeguards**. Article 5(1)(b), Article 6(4), and Article 89(1) together create a balanced system that allows further processing for research purposes without removing accountability mechanisms or weakening transparency obligations.

For these reasons, **the proposed changes risk undermining the effectiveness of the GDPR's safeguards while offering limited benefits in terms of regulatory simplification or legal certainty.** Any reform affecting the scope of research-related exemptions should therefore be subject to careful legislative scrutiny rather than introduced through a simplification package.

SECTION 5.
AUTOMATED DECISION-MAKING
(Article 22 and related recitals)

Why changes to Article 22 affect the architecture of the GDPR

The proposal subtly alters the normative structure of the provision. The current Article 22 is framed as a right not to be subject to certain forms of automated decision-making, followed by narrowly defined exceptions. The proposed wording instead states that such decisions may be based solely on automated processing where specific conditions are met. While this may appear stylistic, the shift from a prohibition with exceptions to a permission with conditions changes the logic of the provision. Automated decision-making risks being framed as generally acceptable provided certain criteria are invoked, rather than as an exceptional practice requiring strict justification. **The current provision of GDPR reflects a deliberate legislative choice to treat such decision-making as inherently high-risk and to permit it only under narrowly defined conditions, coupled with strong procedural and substantive safeguards. The proposal effectively turns this around.**

In this sense, Article 22 operates as a systemic limit on the deployment of automation as a mode of governance. It is designed to prevent the normalisation of automated decisions in areas that directly affect people's rights and life chances, unless strict requirements are met. In a context where automated decision-making systems are increasingly deployed in employment, credit, welfare, and access to essential services, **weakening the safeguards of Article 22 risks normalising forms of automated governance.**

The proposed changes do not formally repeal Article 22. Instead, they r**ecalibrate its conditions of applicability in a way that significantly weakens its constraining function**. As with other amendments in the Digital Omnibus, the issue is not textual deletion but a shift in legal architecture, whereby a provision intended as a barrier to certain practices risks becoming a framework for their routine justification.

The necessity test and its transformation

Under the current GDPR, automated decision-making is permitted in limited circumstances, including where it is necessary for the performance of a contract. **This necessity requirement has consistently been understood as a strict and objective test.** It requires that automation be indispensable to achieving the contractual purpose, not merely efficient, scalable, or economically advantageous.

The proposed changes weaken this logic by reframing how necessity is assessed. The amended text clarifies that automated decision-making may be considered necessary for entering into or performing a contract regardless of whether the decision could be taken otherwise than by solely automated means. **This formulation significantly changes the meaning of necessity within the provision. In doing so, they risk transforming necessity from an external legal constraint into a function of system design.** Where controllers design services around automated decision-making from the outset, automation can be presented as necessary simply because the service has been structured to depend on it. Once the legal test no longer requires demonstrating that alternative decision-making methods exist, necessity risks becoming a function of system design rather than an external legal constraint. This collapses the distinction between what is objectively required and what is organisationally convenient.

As a legal test to protect personal data, a necessity test requires demonstrating that no less intrusive means exist to achieve the same objective. **By stating that automated decision-making may be considered necessary even where the same decision could be taken through other means, the proposal risks emptying the necessity requirement of substantive meaning.** The concept of necessity becomes detached from the existence of alternative decision-making models and instead depends on how controllers choose to organise their systems.

In practice, this is particularly significant in areas such as recruitment, creditworthiness assessments, insurance, access to essential services, and content moderation. **In these contexts, controllers can plausibly argue that large-scale operations require automation, even where alternative models with meaningful human involvement would remain feasible**.

Once necessity is interpreted in this way, Article 22 no longer operates as a limit on automation. It becomes a mechanism through which automation is normalised, and the burden shifts to individuals to demonstrate why automated decisions should not apply to them after the fact. **Such an interpretation would also depart from the strict understanding of 'necessity' developed in EU fundamental rights law**, including under Article 52(1) of the Charter of Fundamental Rights of the European Union.

Contractual justification and circularity

The interaction between automated decision-making and contractual necessity further compounds this risk. **If contractual necessity is assessed by reference to how a service is designed rather than to the nature of the contractual obligation itself, the test becomes circular**. Controllers can structure services around automated systems and subsequently invoke that structure as evidence that automation is necessary. Controllers can define their contractual offering in ways that make automation appear indispensable, thereby satisfying the legal threshold by design rather than by objective assessment.

This circularity undermines legal certainty. Individuals cannot reasonably predict when they will be subject to automated decisions, nor can they effectively contest claims that such decisions are unavoidable. Supervisory authorities, in turn, are left to assess necessity claims in contexts where business models and technical architectures are already structured around automation.

The result is also a **gradual expansion of automated decision-making** through contractual framing, rather than through an explicit and democratically debated policy choice.

Human intervention as a weakened safeguard

Article 22 also relies on the availability of meaningful human intervention as a central protective element. This safeguard is intended to ensure that individuals are not subject to decisions that cannot be genuinely reviewed, explained, or altered by a human decision-maker.

The proposed changes **risk weakening this safeguard by allowing human involvement to be reduced to a formal or procedural step rather than a substantive review**. In complex

AI-driven systems, human intervention often occurs downstream, with limited access to relevant information, limited time, and limited authority to meaningfully alter outcomes.

Where automated decision-making operates at scale, meaningful human review becomes increasingly difficult to implement in practice, even if it is formally provided for. If the threshold for applying Article 22 is lowered while the content of human intervention remains loosely defined, the protection offered by the provision becomes largely symbolic.

In such a scenario, individuals retain rights on paper, but face significant structural barriers to exercising them effectively.

Why this cannot be treated as simplification

Article 22 embodies a core policy choice about the acceptable limits of automation in a rights-based legal order. **Weakening its conditions of application reshapes how power is exercised through digital systems and how risks are distributed between controllers and individuals.**

Such a recalibration cannot be justified through a simplification exercise. If changes to Article 22 are to be considered at all, they require a full legislative process, grounded in a transparent debate about automation, accountability, and human oversight, and assessed in light of their cumulative impact on rights, enforcement, and legal certainty.

SECTION 6.

TRANSPARENCY, ACCESS, AND INFORMATION RIGHTS

(Right of access and right to information)

Why transparency rights are central to the GDPR's architecture

The right of access and the right to information are foundational to the GDPR. They enable individuals to understand how their personal data are processed and provide the entry point for exercising other rights, including rectification, erasure, objection, and the right not to be subject to certain forms of automated decision-making.

The Digital Omnibus does not remove these rights. Instead, **it introduces new conditions, exceptions, and flexibilities that significantly weaken their practical operation**. As in other parts of the proposal, the concern is not formal repeal but structural erosion.

These changes have effects well beyond transparency itself. **When access and information rights are weakened, enforcement becomes more difficult, supervisory oversight less effective, and legal certainty diminished for all actors involved.**

Right of access: from a core right to a conditional mechanism

The right of access under Article 15 GDPR allows individuals to confirm whether their data are being processed and to obtain meaningful information about that processing. It **plays a central role in revealing unlawful practices, discriminatory profiling, and the misuse of personal data across an array of fields**. Access requests are often the only practical tool that allows individuals (with a notable role of workers and their representatives), researchers, and civil society organisations to uncover discriminatory profiling, unlawful automated decision-making, or large-scale data misuse. **Weakening this right therefore affects not only individual transparency but also broader accountability mechanisms within the digital ecosystem.** In many cases, access requests also serve as a practical mechanism for independent scrutiny of digital infrastructures that would otherwise remain opaque, including large-scale advertising and data brokerage systems.

The Digital Omnibus introduces in Article 12(5) additional grounds to refuse, delay, or limit access requests, including references to abuse, excessiveness, or presumed prior knowledge. While safeguards against manifestly unfounded requests already exist in the GDPR, the proposed changes broaden the discretion afforded to controllers.

In practice, **this proposal risks turning the right of access into a conditional mechanism, dependent on controller assessments of intent, proportionality, or burden and, with it, potentially abuse**. Individuals may face refusals without clear criteria, and contesting such decisions becomes more difficult, particularly where information asymmetries are already high.

This erosion of access rights **directly affects legal certainty**. Individuals cannot reliably predict when access will be granted or denied, and SAs face increased difficulty in assessing whether refusals are justified. The result is a weakening of one of the GDPR's most effective enforcement tools.

Right to information and the weakening of rights activation

The right to information under Articles 13 and 14 GDPR is a structural precondition for the exercise of other rights. By ensuring timely and specific information about processing, it enables individuals to understand when the GDPR applies and to activate rights such as access, objection, erasure, and safeguards against automated decision-making.

The Digital Omnibus expands exemptions from information obligations and allows for more generalised or delayed disclosures, particularly in contexts such as research, large-scale processing, or situations deemed disproportionate or impractical. **These changes do not merely affect the level of detail provided but alter the function of the right itself.**

By shifting from specific, *ex ante* information to abstract or deferred disclosures, the proposal **weakens individuals' ability to identify concrete processing activities and legal bases that trigger rights**. This is especially problematic in complex and AI-driven systems, where generic information does not enable meaningful understanding or contestation.

The result is a **displacement of the burden from controllers to individuals**, who are expected to infer when rights apply rather than being clearly informed. In practice, this risks turning the right to information into a formal obligation with limited capacity to support effective rights exercise and enforcement.

Cumulative effects on rights and enforceability

Taken together, the proposed changes to access and information rights **reduce the GDPR's capacity to operate as a preventive and enforceable framework**. Transparency shifts from a proactive obligation to a reactive, conditional process.

This has cascading effects. Without reliable access and information, individuals cannot effectively challenge unlawful processing. **SAs receive fewer complaints grounded in concrete evidence**. Patterns of systemic non-compliance become harder to detect.

This reduction in transparency has **consequences beyond the GDPR itself**. Where people do not receive sufficiently specific and intelligible information about how data are used in AI-supported or automated decision-making contexts, they may also be unable to recognise possible infringements under other areas of Union law, including rules on AI, discrimination, consumer protection, or access to essential services. Information rights therefore do not serve transparency alone. They are a precondition for contestation, complaint, and effective redress across the wider legal framework.

Legal certainty suffers as a result. Rights that depend on discretionary assessments, vague thresholds, or delayed disclosure are difficult to rely on in practice, even if they remain formally enshrined in the law.

Why these changes cannot be justified as simplification

Simplification can clarify procedures or streamline communication. It cannot justify transforming core rights into conditional or discretionary mechanisms. The proposed changes to the right of access and the right to information recalibrate the balance between transparency and convenience in favour of controllers. **This is a substantive policy choice with direct implications for fundamental rights and enforcement.**

If such changes are to be considered at all, they require a full legislative process, supported by a clear policy rationale and an assessment of impacts on rights, legal certainty, and supervisory oversight. In the **specific case of the right to access**, where a controller refuses, delays, or limits an access request on the basis that it is abusive, excessive, repetitive, or concerns information already known to the data subject, that refusal should at minimum be reasoned, specific, and provided within a short and clearly defined timeframe. Otherwise, the individual is denied not only access to data, but also a meaningful opportunity to challenge the controller's assessment or seek an effective remedy.

SECTION 7.
PERSONAL DATA BREACH NOTIFICATION
(Article 33 and related changes)

Personal data breach notification obligations under Articles 33 and 34 GDPR play a central role in accountability and oversight. They ensure that SAs and affected individuals are informed of incidents that may pose risks, enabling timely mitigation and enforcement. The Digital Omnibus proposes to raise notification thresholds and adjust procedural requirements. **While reducing unnecessary reporting may be a legitimate objective, the proposed changes risk undercutting early detection of systemic problems**.

In practice, **higher thresholds shift discretion towards controllers**, who are required to assess risk internally before deciding whether notification is required. In complex or opaque systems, particularly those involving AI or large-scale processing, such assessments are inherently uncertain. This shift **affects legal certainty**. Individuals may

remain unaware of breaches that affect them, and SAs may receive fewer signals of recurring or structural failures. Over time, this weakens both deterrence and trust.

At the same time, **breach notification rules are capable of refinement**. With clearer criteria, stronger documentation requirements, and safeguards against under-reporting, procedural adjustments could be adopted without undermining the protective purpose of the framework. Such changes, however, must reinforce accountability rather than reduce visibility.

SECTION 8.

DATA PROTECTION IMPACT ASSESSMENTS

(Article 35 and related changes)

Data Protection Impact Assessments (DPIAs) under Article 35 GDPR are a core preventive mechanism. They are **designed to identify and mitigate risks before processing begins**, particularly in cases involving new technologies, large-scale processing, or high risks to rights and freedoms. The Digital Omnibus introduces changes that expand exemptions from DPIA obligations and increase reliance on predefined lists or internal assessments. While some clarification may be justified, **the proposed approach could risk weakening the preventive function of DPIAs**.

Where controllers are allowed to rely more heavily on generalised whitelists or abstract risk categories, **DPIAs risk becoming formalities rather than meaningful assessments**. This is particularly problematic in AI-driven and data-intensive contexts, where risks emerge from system design, scale, and interaction effects rather than from individual processing operations.

The proposed changes **also affect legal certainty**. Individuals and SAs may find it harder to predict when a DPIA is required, and prior consultation risks being triggered less frequently, even where risks remain substantial.

The proposal also introduces new implementing powers for the European Commission concerning the establishment of lists of processing operations that require or do not require a DPIA. **Granting the Commission such powers risks weakening the role of supervisory authorities and shifting a key risk-assessment mechanism away from the decentralised enforcement model established by the GDPR.** Decisions about high-risk processing operations require close familiarity with technological developments and real-world processing practices. Supervisory authorities are better placed to identify emerging risks and should therefore retain responsibility for establishing and publishing such lists.

That said, unlike changes to scope or lawful bases, **DPIA-related amendments are not inherently incompatible with the GDPR's architecture**. With tighter conditions, clearer thresholds, and a reinforced role for SAs, adjustments could be considered.
Any such changes should preserve DPIAs as a substantive risk-assessment tool, not a procedural checkbox.

Possible improvements that would support compliance without weakening safeguards

If the objective is to improve legal certainty and reduce unnecessary administrative burden, targeted clarifications could be considered without weakening the preventive function of DPIAs.

For example:

- Clearer EU-level guidance on when a DPIA is required in common high-risk scenarios, particularly in relation to AI systems, large-scale behavioural profiling, and automated decision-making affecting access to employment, credit, housing, or essential services.

- Greater harmonisation of national high-risk processing lists under Article 35(4), coordinated through the European Data Protection Board, in order to reduce fragmentation and provide controllers with clearer expectations across the Union.
- Supervisory authorities should establish and publish their own lists of high-risk processing operations and processing operations that do not require a DPIA. The Commission should not be granted implementing powers in this area, as decisions concerning high-risk processing require regulatory expertise and proximity to enforcement practice.

- Stronger documentation requirements where controllers rely on exemptions or predefined lists to conclude that a DPIA is not required. Such documentation should be available to supervisory authorities upon request.

- Clarification that the establishment of lists of processing operations that do not require a DPIA does not exempt controllers from assessing the risks arising from the specific design, scope, context, and purposes of a processing operation. DPIA lists should not function as blanket exemptions from risk assessment.

These types of measures could improve predictability and reduce unnecessary duplication while preserving the preventive logic of Article 35.