Digital Omnibus on Data

The EDRi guide to EP amendment proposals



EDRi
European Digital Rights

EDRi's assessment of the privacy and data protection-related amendments tabled to the Data Omnibus shows that **the European Parliament faces choices that go far beyond technical simplification.** Many amendments would further weaken the GDPR and ePrivacy framework, including by narrowing the scope of personal data protection, facilitating large-scale data reuse for AI, weakening transparency and access rights, or moving fundamental legal choices into implementing acts and technical standardisation.

But **some amendments also show that simplification does not require deregulation.** Parliament can make the framework easier to use while strengthening people's rights, including through binding privacy signals, more consistent DPIA tools and stronger EDPB coordination.

EDRi considers that **the Digital Omnibus on Data proposal should be rejected as a whole.** If the legislative process nevertheless continues, **the European Parliament should at minimum reject amendments that reduce substantive protections or create new data-use privileges, while supporting measures that genuinely simplify compliance, enforcement and the exercise of people's rights.**

Published by European Digital Rights (EDRi) in November 2026
Authored by: Itxaso Domínguez
Edited by: Chloé Berthelemy
This paper has received substantive input from EDRi members and observers, in particular IT-Pol Denmark, and Privacy International.

Table of Contents

4 Executive summary

13 The entry point to the GDPR (aka the spurious debate around the definition of personal data)

19 AI and legitimate interest: no privileged lawful basis for AI

22 Scientific research: genuine research or a general data-reuse route?

26 'Sensitive' data and biometrics: AI should adapt to Article 9, not the reverse

29 Automated decisions: efficiency is not the same thing as necessity

33 Access and information: rights should not depend on why a person asks

36 Keep terminal-equipment confidentiality in ePrivacy

41 Privacy signals: the clearest test of whether simplification is real and rights-respecting

45 When simplification becomes an excuse to rewrite the GDPR

53 Acronyms

1. Executive summary

In November 2025, the European Commission presented the Digital Omnibus as an exercise in 'simplification': a package intended to reduce regulatory complexity, lower compliance costs and make the EU's digital rulebook easier to apply. The Digital Omnibus was divided into two main strands. One reopened the Artificial Intelligence Act and has since been adopted as Regulation (EU) 2026/1744. The other - the Digital Omnibus on Data or 'Data Omnibus,' which is the subject of this paper - proposes changes across a wide range of EU data and digital laws, including the General Data Protection Regulation (GDPR), the EU institutions' data-protection regulation (EUDPR), the ePrivacy Directive, the Data Act and other parts of the EU Data Acquis[1], as well as rules on cybersecurity incident reporting. It would also repeal several existing instruments, including the Platform-to-Business Regulation. **The Commission describes these changes as 'targeted simplification' intended to allegedly preserve existing levels of protection.**

Much of the Data Omnibus goes considerably further than harmless simplification: it reopens fundamental choices about when the GDPR applies, what companies may do with 'sensitive' data, whether AI development should receive special legal privileges, when consequential decisions may be automated, how people can find out what is being done with their data, and whether access to their devices remains protected by the confidentiality logic of ePrivacy. The overall effect is to water down established rights and legal protections. It also raises a less visible but equally important question: courts ultimately interpret EU law, and independent supervisory authorities and the EDPB are responsible for supervision and consistent application of the GDPR. The Omnibus debate is increasingly about who gets to set the detailed rules that shape those boundaries in practice: the legislature and courts, independent data-protection bodies, the Commission through implementing acts, technical standardisation bodies where industry is heavily represented, or regulated actors themselves.

These changes arrive only a few years after many of the relevant rules were agreed and, in some cases, before their implementation and enforcement have had time to mature. They also form part of a wider EU 'simplification' agenda in which rights and safeguards are increasingly described as regulatory burdens. **'Simplification' became a shortcut for reopening political compromises, expanding exceptions or shifting responsibility away from the actors that collect and use data and onto the people affected by them.**

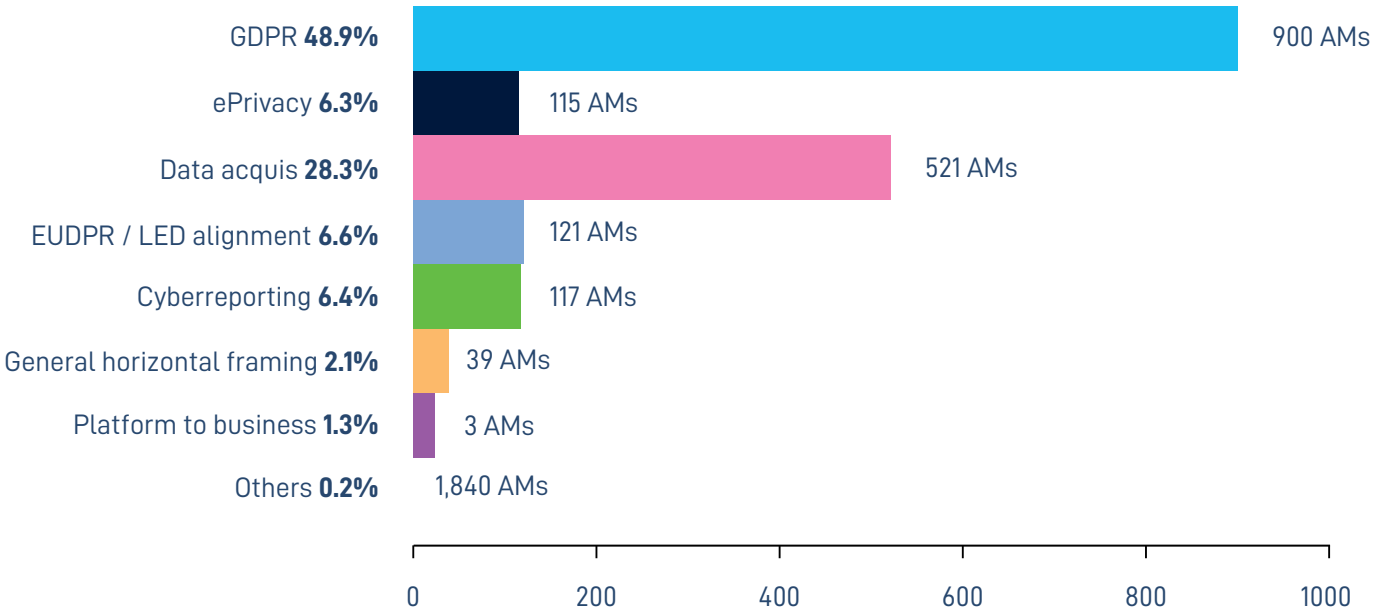
The central question of simplification

Does a proposed simplification remove duplicated procedures and make compliance or the exercise of rights easier, or does it change the substantive condition under which a right, duty or legal limit applies? The former should be considered, the latter rejected.

1. In this guide, 'EU Data Acquis' refers to the body of EU rules governing access to, sharing, reuse and governance of data. In the Commission proposal this includes, in particular, the Data Act, Data Governance Act, Open Data Directive and Free Flow of Non-Personal Data Regulation, with those rules being consolidated into the Data Act.

The legislative process is now testing exactly that distinction. In the European Parliament, Members have tabled 1,840 amendments: 78 changes contained in the joint LIBE–ITRE draft report, counted together with the 1,762 further amendments tabled afterwards by MEPs.

Distribution of the 1,840 amendments to the Digital Omnibus on Data, including the 78 amendments in the joint LIBE/ITRE draft report and the 1,762 subsequently tabled by MEPs



The amendment stage has turned the Data Omnibus into a much wider argument about what EU data protection and privacy should become. Some amendments try to restore the safeguards weakened by the Commission proposal. Others go considerably further than the Commission in deregulating data use. Even some contain genuinely useful ideas for reducing complexity without reducing protection. Meanwhile, Member States agreed on their own negotiating position – the so-called 'General Approach' - under the Irish Presidency on October 21st, 2026, in a text that ultimately contributes to the deregulatory drive initiated by the European Commission.

BEYOND SIMPLIFICATION: WHAT PARLIAMENT IS ACTUALLY DECIDING

- When does the GDPR apply, and who gets to decide when data falls outside it (and hence, when our rights are no longer valid)?
- Should AI receive special routes around ordinary rules on purpose limitation, legitimate interest and sensitive data?
- When may consequential decisions be automated, and what counts as necessity and meaningful human intervention?
- Can people still find out what is being done with their data and challenge it without having to justify why they are asking?
- Will access to a person's device remain protected by a distinct and more protective confidentiality rule, or be folded into GDPR lawful-basis logic?
- Who sets the practical boundaries of compliance: the legislator and courts, independent data-protection authorities and the EDPB, the Commission, standardisation bodies where industry is heavily present and influential, or regulated actors (companies) themselves?

These choices matter more than the sheer number of amendments. Together, they determine what kind of data-protection framework will emerge from this Omnibus.

This guide aims to help Members of the European Parliament and other decision-makers, along with the wider public whose rights are at stake, navigate that amendment landscape. It asks what the competing amendments would mean in practice, which regulatory model they would create, and whether they make EU digital rules simpler while protecting people, or simpler mainly for organisations that want to collect, reuse and monetise more data oftentimes violating our rights. For this, it focuses on the amendments that affect the GDPR, ePrivacy and closely related questions of data-protection and privacy governance. It does so by grouping amendments by the legal problem they address and, where relevant, reads them as political packages rather than isolated drafting changes.

Recommendations

This phase of the legislative process gives Parliament an opportunity to draw a clear line. Simplify procedures, remove unnecessary duplication and make rights easier to exercise. Do not simplify away the rights themselves. **Taken together, the amendments show that Parliament does not face a binary choice between a complicated GDPR and deregulation. There are amendments that could genuinely make the rules easier to use: binding privacy signals, clearer and more consistent DPIA tools, stronger EDPB coordination, streamlined reporting mechanisms and better allocation of responsibility to powerful processors. Those proposals demonstrate what simplification can look like when its objective is to make rights and obligations work better.**

The alternative emerging from other parts of the amendment spectrum is very different: narrower GDPR scope, special legal pathways for AI, new sensitive-data exceptions, broader consent-free device access, weaker transparency and greater reliance on controllers, standards or executive acts to decide when safeguards apply. That may make some forms of data exploitation easier. It does not make European digital regulation simpler in any meaningful sense.

- **Do not rewrite the definition of personal data – directly or indirectly - to create new routes out of the GDPR**. Identifiability is already contextual under the GDPR and Recital 26. Parliament does not need to manufacture a new actor-by-actor classification system in which the same information can move in and out of GDPR protection depending on how a company organises access to identifying information. The issue is not whether relativity exists, but whether organisational design - who holds a key, which affiliate receives a dataset, who is contractually forbidden from linking it - becomes a clearer way for individual actors to place processing outside GDPR scope. Support amendments that delete or neutralise the actor-relative rewrite (AMs 928–932 and 934–936; related Recital 27 AMs 211–232) and deletion of Article 41a (AMs 1243–1248 and 1250).

- **AI does not need privileged access to personal or 'sensitive' data,** and Parliament should reject a dedicated legitimate-interest route for AI development and operation: Article 6(1)(f) already exists and can apply where its ordinary conditions – the three step-test - are genuinely met. Nor should the difficulty of filtering 'sensitive' information from huge AI datasets become a reason to lower Article 9 protection. Support deletion of the AI-specific legitimate-interest route (AMs 1551–1556, 1559 and 1577; related Recital 30 AMs 251–268 and Recital 31 AMs 269–280) and deletion of the AI-specific Article 9 derogation (AMs 1018–1023; related Recital 33 AMs 296–310).

- **Automated decision-making should remain genuinely exceptional, not merely efficient.** A company's preference for a cheaper, faster or more scalable automated decision is not the same as legal necessity, and nominal human involvement is not meaningful review. Support amendments restoring a strict contractual-necessity test and meaningful human review (including AMs 1142, 1147–1151, 1153, 1155 and 1161; related Recital 38 AMs 360–377).

• **Access and transparency are not administrative luxuries** because they correct a structural information imbalance. The right to know what information an organisation holds, where it came from and how it is being used is often the only way people, workers, journalists, trade unions and civil-society organisations can discover unlawful profiling, discrimination or hidden automated processing. Support amendments removing motive-based restrictions and preserving the controller's burden of proof (including AMs 1080, 1093–1094 and deletion AMs 1116–1121; related Recital 35 AMs 323–334 and Recital 37 AMs 350–359). Administration can be simplified without making rights harder to exercise.

• **So-called 'cookie fatigue' should be solved by letting people communicate a durable choice once,** not by making more tracking consent-free. Binding privacy signals are one of the clearest examples in the whole file of genuine simplification: they can remove repeated interfaces while strengthening, rather than removing, people's choices. The amendment pattern strongly suggests that a parliamentary majority supports retaining a privacy-signal mechanism in some form, even though MEPs disagree sharply over its legal effect, technical design, scope and timing. The total-deletion amendments are concentrated in one amendment family, while several other packages keep Article 88b and argue over its modalities. Support binding, interoperable privacy signals and the duty to respect them (including AMs 1493–1494, 1516, 1534–1535 and 1540–1541; related Recital 45 AMs 458–462 and Recital 46 AMs 463–477), while deleting the media exemption (AMs 1496–1503).

• **Protect children by making services safer, not by making everybody prove their age and identity.** Several amendments add meaningful protections for children, but those protections should be designed around services and processing likely to involve or affect children (for example AMs 1131, 1160 and 1173), rather than forcing every user to demonstrate whether they are an adult. Amendments that normalise 'privacy-preserving age assurance' still raise a prior question: why should age assurance be required in the first place?

Main findings

Three differeny paths available to parliamnt

• Some amendments restore current GDPR or ePrivacy safeguards, and even some attempt at strengthening them. These are the clearest rights-protective amendments.

• Some improve a problematic part of the Commission proposal without restoring current rights protection. These could be important fallbacks if the underlying provision survives, but they should not be considered as a rights-strengthening end state.

• Others go beyond the Commission proposal and create new exclusions, permissions, safe harbours or institutional shortcuts. These are often the amendments that most clearly show how a 'simplification' file can become a vehicle for even more substantive deregulation.

Where lie the main dangers?

• The most dangerous battles for digital rights concern the boundaries of the GDPR and AI data reuse. The most concerning packages address the definition of personal data and the proposed AI-specific legitimate-interest route. Both debates would change the conditions under which the GDPR applies or large-scale data reuse becomes easier.

• MEPs seem to be somehow more protective on automated decisions, access, information and DPIAs. The amendment pool contains substantial efforts to restore a strict Article 22 necessity test, protect access and transparency, and keep DPIA standard-setting with independent data-protection bodies.

• ePrivacy is the most fragmented battlefield. Some amendments preserve a single equipment-access rule in ePrivacy, strengthen confidentiality and make privacy signals binding. Others create broader consent-free tracking routes, sectoral carve-outs or remove the signal mechanism altogether. The result is as much a debate about legal architecture as one about cookies and other tracking technologies.

Simplification is possible!

• Some amendments contain real simplification ideas that do not require weaker rights. Examples include common DPIA tools and integrated assessments that preserve the high-risk trigger (AMs 58 and 1235; related Recital 40 AMs 388–394), pooled or shared DPO arrangements for smaller organisations (AMs 349, 1239, 1241 and 1242), clearer complaint pathways (for example AM 1341), and binding privacy signals that let people express a durable choice once (for example AMs 1493, 1516 and 1534–1541; related Recital 46 AMs 463–477). These proposals reduce friction by making compliance and rights easier to exercise and are a useful benchmark for the rest of the Omnibus: simplification should remove duplication and manipulation, not remove the underlying safeguard and the rights on which these laws were built.

Who should set the practical rules?

• Several amendments go far beyond alleged technical assistance also in terms of institutional decision-making. AMs 1254, 1267, 1280, 1282–1285 and 1293 would give Commission-made criteria, methodologies, codes, certification or common measures a larger role in deciding whether data are anonymous or processing is compliant; AMs 1159 and 1170 similarly give technical specifications or certified PETs special legal weight. AM 1096 would even allow the Commission to specify criteria for when an access request is 'manifestly unfounded or excessive.' The concern is not that the Commission may never adopt implementing rules. It is that implementing acts may specify only non-essential elements within the limits set by the legislature. They cannot be used to redefine the essential scope of a fundamental-rights law, narrow Charter protection, or substitute executive criteria for the legal tests that courts and independent supervisory authorities must apply. Harmonisation can help, but the practical boundary of a right cannot be rewritten through a technical rulebook.

Issue	Current legal anchor	Shift proposed in parts of the amendment pool	Why it matters
Scope / anonymisation	GDPR, CJEU case law, EDPB and DPA interpretation	Commission criteria, codes, certification or actor-led assessments	These mechanisms can influence whether the GDPR applies at all
DPIAs	Risk test, DPA lists and EDPB consistency mechanism	More centralised lists, templates or adoption roles	Harmonisation can help, but the institution setting the threshold can shape when preventive scrutiny is required
Privacy signals	Legal rules on consent, objection and withdrawal	Standardi-sation and technical inter-mediaries	Standards should implement legal choices, not decide what a refusal or consent means
PETs and certification	Risk-mitigation safeguards within ordinary GDPR duties	Presumptions, safe harbours or privileged processing	A technical safeguard can reduce risk without answering the prior question of whether the processing is lawful
Access-right limits AM	Article 12 GDPR, CJEU case law and independent supervisory authorities	Commission implement-ing-act criteria for 'manifestly unfounded or excessive' requests	Criteria that determine when access can be refused or charged directly shape the practical scope of a Charter-linked right

The PETs mirage

• Privacy-enhancing technologies are increasingly invoked as a general answer to legal and regulatory concerns, and the amendment pool contains several versions of that move. AM 228 promotes a catalogue of PETs but couples it with Commission technical criteria. AM 1159 would let the Commission set PET specifications across pseudonymisation, anonymisation, legal-basis and risk questions. AM 1170 would create a rebuttable presumption of compliance with data minimisation for certified PETs. AMs 1405, 1408, 1410-1411 and 1413 go further by using PETs as part of new consent-free routes to terminal equipment or by asking the Commission to determine when risk mitigation is effective. AM 1576 outsources minimum anonymisation and abstraction standards for AI to standardisation bodies. AM 1604 would automatically treat further processing undertaken solely to anonymise data as compatible with the original purpose. What is critical to understand is that promoting strong PETs can be useful, but giving a technology the legal effect of a permission, safe harbour or presumption is much more problematic: pseudonymisation does not create a lawful basis, encryption does not make an incompatible purpose compatible. Aggregation is not necessarily anonymisation. The sequence should remain legal first, technical second: establish that processing is lawful, necessary and proportionate, then use the strongest verifiable PETs to reduce the residual risk.

Risk-based, or rights-conditional?

• Several amendment packages propose a more explicitly risk-based architecture. Recital AM 224 and operative AMs 923, 924, 926 and 1098 create size- and risk-based categories that can reduce duties or remove processing from the GDPR. AMs 295 and 1597 use the industrial context as a proxy for lower risk and then disapply a substantial set of rights and accountability duties. Other proposals use certification or Commission-made criteria to determine lighter treatment. The GDPR already uses risk and proportionality throughout its accountability architecture. The key distinction is whether risk calibrates how a controller complies, or whether a controller's classification switches off a person's right or a legal safeguard. The first can be legitimate. The second makes fundamental rights conditional on a controller's own risk category and can reward under-classification.

The privacy-signals battle

• Automated privacy signals are the clearest test of whether the Omnibus genuinely wants to reduce banner fatigue. A binding signal lets a person express a durable choice once. The strongest amendment packages add withdrawal and more granular choices (AMs 1469-1472, 1476, 1478 and 1482-1484), give the signal binding legal effect and prevent repeated requests (AMs 1493-1494), remove a presumption of lawfulness based on technical standards (AMs 1516 and 1518), and require interoperable support across browsers, applications and operating systems with room for independent agents (AMs 1534-1535 and 1540-1541). The weakest approach is total deletion of Article 88b (AMs 1443-1454). Other amendments do not delete signals but weaken them, for example by making the mechanism voluntary or deleting parts of the choices in paragraph 1 (AMs 1455, 1459-1462 and 1466-1468), or by deleting the controller's duty to respect signals (AMs 1488-1491). This distinction matters

politically: the amendment pool is not evenly split between 'signals' and 'no signals,' and most competing models retain a signal architecture and fight over its strength.

Strange bedfellows?

• This guide identifies several areas where amendments with a rights-protective legal effect are sponsored by actors with very different political projects, including progressives and far-right (who, to be sure, combine rights-protective amendments with very substantial deregulatory proposals) or non-attached MEPs. This should not be presented as a shared political coalition, because deletion can protect the GDPR for one sponsor and express hostility to EU regulation, and with it rights, for another.

Who gains, who loses?

• Legal uncertainty does not create a level playing field. It shifts power towards the actors best equipped to navigate it. If the applicability of the GDPR increasingly depends on contested questions about identifiability, pseudonymisation, technical safeguards, standards or the capabilities of particular actors, then people first have to establish that the law applies before they can even invoke the rights it gives them. Civil-society organisations and trade unions face the same problem when trying to investigate systemic practices, and regulators may have to spend more time resolving threshold disputes about scope before they can examine whether the underlying processing is lawful. That means more factual investigation, more technical expertise and more litigation simply to reach the starting line, that is, a rights-respecting one.

• Nor should actor-relative GDPR scope, PET-based presumptions or Commission-made criteria be sold as an automatic benefit for SMEs. A small publisher, retailer, transport operator or app developer may remain the company that people see and complain to, while relying on much larger cloud, analytics, advertising or AI providers further down the chain. Those providers may be in a much stronger position to argue that the pseudonymised data they receive are not personal data for them, that a particular PET sufficiently reduces risk, or that a standard or certification supports their interpretation. The smaller business can – and will - therefore remain exposed to compliance duties and reputational risk while having very limited visibility over, or bargaining power against, the infrastructure provider on which it depends.

• The actors that benefit most from ambiguity are generally those that can afford to turn ambiguity into a strategy: Big Tech platforms, dominant cloud and infrastructure providers, major adtech companies and large AI developers. They have specialist legal teams, technical expertise, standard-setting capacity and the resources to sustain years of regulatory disputes or litigation. They are also much better placed to design processing architectures around favourable interpretations of the law and to influence the technical standards that may later be used as evidence of compliance, whereas a small organisation rarely has those options.

• In that sense, weakening clear legal boundaries does not truly 'reduce burdens,' and it can actually redistribute them: away from the companies with the greatest technical and legal capacity, and towards people who have to prove their rights apply, civil society that has to uncover opaque practices, regulators that have to

litigate basic questions of scope, and smaller businesses that remain dependent on infrastructure they do not control. The result will be less legal certainty for everyone except those large enough to manage uncertainty as part of their business model that structurally abuses rights.

2. The entry point to the GDPR

(aka the spurious debate around the definition of personal data)

Article 4(1), proposed Article 41a GDPR + Omnibus Recital 27
Simplification verdict: this is not simplification. Changing when an organisation can place data outside the GDPR does not simplify compliance but changes whether the rights and duties exist in the first place

+

928-932, 934-936 Delete/neutralise the Commission's new actor-relative subjective approach in Article 4(1).

1243-1248, 1250 Delete proposed Article 41a and its Commission implementing-act machinery.

1253, 1264, 1266, 1272 Shift interpretative weight towards the EDPB or removing parts of the Commission's role.

−

940 Keeps the possibility that information is non-personal for an entity that cannot identify the person, but introduces a downstream qualification.

942 Creates a specific rule for trained AI-model parameters where the person cannot be identified from the model. It is unclear whose capabilities count and it risks conflating model output with the controller's wider capacity to identify

941, 943, 944 Retain and/or build on the problematic actor-relevant approach

946–948 Go even further in the wrong direction than Commission proposal by creating new routes out of scope for transitory/technical processing, enterprise/object data or certain inferred health data.
1169 and 1605
Create an actor-relative route, reproducing the actor-relative approach through a new definition.

1249 Creates an unsafe 'instant anonymisation' route and switches off Article 9 where processing is solely for immediate anonymisation.

1254, 1267, 1280, 1282–1285, 1293, 1159, 1170, 1273, 1287 Expand criteria, methodologies, codes, certification or common measures that can influence GDPR scope or compliance, including in relation to PETs'.

1287, 1289 Give technical or organisational separation greater weight in treating pseudonymised data as outside the GDPR.

1302 Gives the EDPB a stronger role but still allows pseudonymised data to become non-personal for particular recipients.

Why this matters

The definition of personal data in article 4(1) is the entry point to the GDPR. If information falls outside that definition, then the GDPR's rules on lawful basis, transparency, access, objection, security, DPIAs and accountability do not apply to that processing at all. **This is therefore a question about whether people receive GDPR protection at all.**

The Commission has proposed to add an explicit actor-relative rule directly to Article 4(1) GDPR. Today, Recital 26 already requires identifiability to be assessed in context, taking account of objective factors such as cost, time, available technology and the means reasonably likely to be used, either by the controller or another person The Commission's wording goes much further by expressly stating that information may be personal data for one entity but not for another, depending on the means reasonably likely to be available to each. It also says that the fact that a later recipient could identify the person would not, by itself, make the data personal for the first entity. This wording contradicts Recital 26 and CJEU case law.

The proposal does not add legal certainty. Recital 26, CJEU case law and existing EDPB work already provide contextual tests for identifiability and risk. The EDPB's Guidelines 01/2025 on Pseudonymisation already addressed when pseudonymised data remain personal data and how pseudonymisation affects risk and compliance. Its Guidelines 02/2026 on Anonymisation, adopted for public consultation in July 2026, address the separate and higher threshold for data to become anonymous. Adding a new actor-relative statutory rule, plus Commission criteria under Article 41a, creates another layer of threshold disputes instead of resolving them. Legal certainty comes from a stable legal test applied consistently, not from multiplying routes by which the same dataset may change legal status between actors. Many tabled AMs follow that same dangerous route of contributing to legal uncertainty.

Practical example: Company A passes a dataset containing persistent user identifiers to Company B. Company B does not have the information needed to connect those identifiers to particular people and argues that the GDPR therefore does not apply to it. Company C, receiving the same data later or combining them with information it already holds, may be able to identify the individuals. The Commission's proposal would expressly allow the legal status of the same information to differ between those actors, raising difficult questions about where GDPR protection starts and stops across the data chain.

The enforcement problem

This also creates a chicken-and-egg problem for enforcement and accountability. To discover what data an actor holds, how those data are linked and who receives them, a person may need to make a request under Article 15. But the actor can refuse the request by saying the data are 'not personal for us,' even if the data subject submits a means of identification as foreseen by Article 11(2), e.g. a cookie identifier. The information needed to challenge the classification can therefore be placed behind the classification itself.

A distributed internet founded on humongous supply chains

Supply chains as the foundation of today's distributed internet make the problem harder. A smaller controller may remain the visible organisation that people contact, while a larger analytics, cloud, advertising or AI provider further down the chain argues that the pseudonymised data – and pseudonymised data are commonplace in distributed data chains - it receives are outside the GDPR for it. That can create uncertainty over responsibilities precisely where bargaining power and technical visibility are already uneven.

Legal ConceptPseudonymisation ≠ anonymisation

Pseudonymisation and anonymisation are not the same. Pseudonymisation removes or separates obvious identifiers - for example replacing a name with a code - but leaves a route by which the information can still be attributed to a person with additional information. It is a valuable safeguard, but pseudonymised data remain within the GDPR where identification is still reasonably likely. Anonymisation is the much higher threshold: the person is no longer identifiable in the relevant context, and only then does the information fall outside the GDPR. And it is important to understand that companies rarely want truly anonymous data: once data are genuinely anonymous, much of the individual-level value that powers tracking, profiling and personalisation disappears. The more useful a dataset remains for following, distinguishing or linking people, the harder it is to pretend it is really anonymous.

What do the amendments say?

The LIBE/ITRE Draft Report does not amend the Commission's proposed changes to the definition of personal data or its pseudonymisation architecture, the co-rapporteurs leaving this central part of the Commission proposal untouched.

AMs 928-932 and 934-936 are the preferred solution: leave Article 4(1) alone. The point is not to deny that identifiability is contextual; Recital 26 of GDPR already says it is. The concern with the Omnibus is not recognising context: it is turning that contextual assessment into an actor-by-actor exit from the Regulation and, with it, making organisational choices about who holds identifying information a clearer route out of the GDPR. AM 217 also moves in a useful direction at recital level: it says that the threshold for personal data must remain objective and that pseudonymised data which can still be attributed to a person remain personal data across the processing chain. That recital can support the right interpretation, but it should accompany deletion of the new Article 4(1) wording rather than compensate for keeping it.

AM 940 is a good example of an amendment that can sound reasonable while still changing the logic of the GDPR in a dangerous way, an amendment that improves the Commission's proposal but still represents a danger of weakening rights compared to the current Article 4(1) GDPR. It tries to reassure by saying that data remain personal where the current holder is likely to share them with someone who can identify the person. That sounds like a safeguard against obvious outsourcing tricks. However, the basic rule is still actor-relative: the question becomes whether this controller, or a sufficiently foreseeable recipient, can identify the person. That is much narrower than asking whether the person is identifiable in the real data environment. Identification may depend on several actors combining information, may become possible only later, or may never involve knowing someone's civil name at all: a person can still be persistently singled out, tracked, profiled and acted upon. The danger is that data could be classified as non-personal at an early stage of the chain and lose GDPR protection before those later links become visible. Once that threshold decision is wrong, all the rights and safeguards that depend on the GDPR applying disappear with it.

Other amendments actively and dangerously create new routes out of GDPR scope. AM 942 is AI-specific: it says trained model parameters are not personal data where a person whose data were used in training cannot be identified from the model by means reasonably likely to be used. The amendment does not say clearly whose means are relevant: the model provider's, a deployer's, a recipient's, or another actor's. That ambiguity is especially serious because a model's outputs may reveal or reproduce information about individuals even where direct extraction of a training record from the parameters is difficult. Whether model parameters or outputs constitute personal data is a fact-sensitive application of the ordinary Article 4(1) and Recital 26 tests. Parliament should not create an AI-specific statutory exclusion that pre-judges that analysis or ignores identification through model use and output.

AMs 946 and 947 do even more dangerous damage to the GDPR's structure. AM 946 would let admittedly personal - even 'sensitive' - data fall outside the Regulation where processing is transitory or technical and not 'related' to the person in the amendment's sense. AM

947 focuses on data about an enterprise or object and says a person's mere connection as employee, owner or similar relation should not necessarily make it personal. That is dangerous for industrial and workplace data: machine telemetry, vehicle records, badge logs or production-system data can simultaneously describe an object and reveal where a worker was, what they did, how fast they worked or whether they complied with a procedure. The GDPR already asks whether the information relates to an identifiable person; it does not need an 'object first' escape route.

Tips for the Guide: Read the packages, not just the amendment numbers

Many amendments only make sense when read together. This is particularly important for pseudonymisation. A recital amendment may look protective while an operative amendment still creates a route out of GDPR scope. Article 4(1), proposed Article 41a and any new pseudonymisation rule therefore have to be read as a package. For example, AM 1169 creates an actor-relative pseudonymisation rule and should be read with the Article 41a packages that decide who can set criteria for when the data cease to be personal. Likewise, AM 1253 only makes sense together with AMs 1261-1264, 1266, 1272, 1286, 1295 and 1299, which shift the package away from binding Commission scope-setting and towards an EDPB opinion and existing governance tools. The practical tip is simple: do not judge an amendment number in isolation. Check what happens to the various issues affected by the proposal.

One important point is that the debate goes beyond Article 4(1) GDPR. Other amendments pursue the same actor-relative logic through rules on pseudonymisation, anonymisation, recipient circumstances and technical measures. AM 1169, for example, creates a new Article 29a under which pseudonymisation could mean that data are personal for one actor but no longer personal for another, depending on that recipient's ability to identify the person – it comes very close to restating the current criteria for identifiability (means reasonably likely to be used, by the controller or another person) but doesn't add anything in terms of legal clarity, and includes the possibility of European Commission's Implementing Acts. AM 1605 takes a similar approach by defining anonymisation relative to the particular controller or recipient. Both risk turning technical and organisational separation into a route out of the GDPR, allowing the same dataset to move in and out of protection depending on who holds it and what identifying means they are considered to have. Introducing different tests for identifiability, e.g. depending on whether the personal data has undergone pseudonymisation or not, makes compliance with the GDPR more complicated for controllers, contrary to the Digital Omnibus' stated objective of simplification.

This is one of the areas where the debate over PETs needs understanding. Pseudonymisation, encryption and other PETs should be encouraged because they potentially reduce exposure and help fulfil data minimisation, security and accountability duties. But their use does not in and of itself decide whether data are anonymous, whether Article 6 provides a lawful basis, whether Article 9 permits processing or whether a purpose is compatible. AM 1249's (together with AM 225) 'instant anonymisation' route is a good example of the mistake: sensitive personal data remain sensitive personal data during the processing needed to anonymise them. The lawfulness of that processing has to be

established before the output becomes anonymous. In a similar vein, AM 1170 inserts new paragraphs 3a and 3b into Article 25, creating a rebuttable presumption of compliance with data minimisation where processing is carried out exclusively through certified PETs, and then empowers the Commission to recognise PETs and set certification criteria and standards. As mentioned above, PETs can reduce risks substantially, but certification should not become a substitute for asking whether the processing is actually necessary and limited to what is needed in the specific context.

Who gets to decide?

Proposed Article 41a adds a second layer to a question that determines whether the GDPR applies at all. It would let the Commission adopt criteria and categories for when pseudonymised data may no longer count as personal for certain actors. That is not merely technical guidance. The legislature may empower the Commission to specify non-essential details, but it cannot delegate away the essential elements of the GDPR or allow an implementing act to narrow the protection guaranteed by Articles 7 and 8 of the Charter. If an implementing act can decide, in practice, that whole categories of processing fall outside the Regulation, the executive is no longer merely implementing the law. It is determining the reach of the right and duty structure that the legislature enacted. Harmonised technical advice can help. The legal threshold itself must remain in the legislative act and subject to independent supervision and judicial interpretation.

A parallel institutional fight sits in Article 41a. AMs 1243-1248 and 1250 delete the proposed Commission machinery altogether, and that should be the prefered option. Several fallback amendments instead transfer interpretative weight towards the EDPB or remove parts of the Commission's role: AM 1253, read with AMs 1261-1263, is safer than the Commission model because it moves away from direct Commission scope-setting and towards an EDPB opinion and the existing code-of-conduct framework. But the EDPB already has a broad power under Article 70(1)(e) to examine questions concerning the application of the GDPR and issue guidelines, recommendations and best practices. If Article 41a survives, an EDPB-centred fallback is preferable to Commission-made criteria, but it should not become a shortcut for deciding when the Regulation stops applying.

That EDPB-centred direction is preferable to AMs 1254, 1267, 1280, 1282-1285 and 1293, which would give Commision criteria, methodologies, codes, certification or common measures increasing evidentiary weight in deciding whether data are anonymous or processing is compliant. The EDPB is better placed to provide technical interpretation because it is the independent Union body created by the GDPR to ensure consistent application of data-protection law and brings together national supervisory authorities with enforcement experience. The Charter point is also concrete: Article 8(3) requires compliance with data-protection rules to be subject to control by an independent authority. If Commission implementing acts can effectively determine when information falls outside the GDPR, executive rule-making starts shaping whether that independent-control guarantee applies at all.

Legal Concept - Personal, pseudonymised and anonymous data

Personal data are information relating to an identified or identifiable natural person. Pseudonymisation is a technique applied to personal data that makes it impossible to attribute the data to a specific person without additional information, for example by replacing a name with a code and keeping the information needed to reconnect that code to the person separately and securely. Anonymous information falls outside the GDPR only where the person is no longer identifiable, taking into account the means reasonably likely to be used in the relevant context.

3. AI and legitimate interest: no privileged lawful basis for AI

Proposed Article 88c GDPR + Omnibus Recitals 30 and 31
Simplification verdict: clarifying the existing 'Legitimate Interest test' could improve legal certainty, but creating an AI-specific legitimate-interest route does something different: it gives one technology a privileged legal pathway and makes large-scale reuse easier. That is a substantive change, not simplification

+

251-256, 269-274 Delete/correct the accompanying recital on AI processing and legitimate interests.

1551-1555 Delete Article 88c entirely.

1559 Delete Article 88c(1), removing the core AI legitimate-interest rule.

1560, 1572 Fallback safeguards around information/actions and administration of objections.

−

294 States that AI training can constitute a legitimate interest.

1561 - 1562 Preserve an AI-specific legitimate-interest route, broaden it towards third-party, GPAI or public-authority processing, and remove the national-law consent caveat.

1563- 1564, 1566-1567 Broaden the route to training, testing, validation, deployment, monitoring, third-party interests or GPAI.

1581, 1584, 1587, 1589 Strip back minimisation or the unconditional objection safeguard.

1595 Creates a broad catalogue of legitimate interests including workplace monitoring and development of new technologies/AI.

Why this matters

Article 6(1)(f) GDPR already allows processing for a controller's legitimate interests where three conditions are met: there is a genuine legitimate interest; the processing is necessary for it; and that interest is not overridden by the person's interests, rights and freedoms. AI developers are not prevented from relying on Article 6(1)(f) of the GDPR. Where the three conditions are met, AI-related processing can already proceed on the same basis as any other form of processing.

However, the Omnibus creates Article 88c, expressly recognising not just AI development, but also operation (potentially a much broader set of operations), as a context in which legitimate interests may be pursued. That matters even if the normal balancing test formally remains. **A dedicated AI article sends a legal and political signal that AI is a specially favoured context in an otherwise technology-neutral framework.** Once the clause exists, amendments can expand it to third-party interests, general-purpose AI, public-authority tasks or weaker objection rights, which is exactly what several tabled amendments do. The dedicated provision creates a presumption-like legislative signal that AI-related processing is a specially recognised legitimate interest context, even though the ordinary Article 6(1)(f) test formally remains.

Legal Concept - Legitimate interest is a three-step test

Article 6(1)(f) does not simply ask whether a controller can name an interest. The controller must identify a legitimate interest, show that the processing is necessary for that interest, and balance it against the person's interests, rights and freedoms. While Article 88c does not formally remove those requirements, it would expressly identify AI development and operation as activities capable of pursing legitimate interests. In doing so, it risks shifting the starting point of the analysis. Rather than assessing the legitimacy of AI-related processing in the same way as any other processing activity, controllers may treat AI as legislatively-endorsed and this may also influence how the remaining stages of the test are applied.

What do the amendments say?

The LIBE/ITRE draft report does not amend the Commission's proposed AI-specific legitimate-interest provision, the rapporteurs leaving the core Commission approach intact at draft-report stage, rather than deleting or narrowing the dedicated route.

AMs 1551-1555 delete the proposed provisions and therefore remove a technology-specific privilege (related Recital 30 AMs 251–268 and Recital 31 AMs 269–280). Controllers processing data for AI-related purposes would then remain under the same ordinary GDPR framework as controllers processing data for other purposes: Article 6(1)(f) may be used where its three conditions are genuinely met, without a special statutory signal favouring AI.

If Article 88c is not deleted, several amendments provide materially better fallback safeguards. In this regard, AM 1569 is worth distinguishing from the more aggressive expansions: it moves towards a generic, case-by-case legitimate-interest formulation and avoids some of the presumption-like language. Read with Recital AM 250 and AM 1015, it moves towards codifying the existing three-step legitimate-interest test: a real and lawful interest, necessity including less intrusive alternatives, and balancing against rights and reasonable expectations. That could be a better fallback direction, but the simplest and most legally coherent solution remains to delete Article 88c and rely on Article 6 itself. Similarly, AM 1015 is broadly useful, although its reference to mitigating measures should not be read as allowing safeguards to rescue processing after the balancing test has already failed. AM 1560 adds concrete AI safeguards, including an absolute objection, anonymisation where possible, abstraction, leakage testing and the ability to honour data-subject rights. AM 1572 adds specific transparency about the actions taken under the safeguard paragraph. AM 1580 adds minimisation, controls on inference, extraction and regurgitation, enhanced transparency and an unconditional objection. These are damage-limitation measures, not a reason to keep the privileged AI route, but they are preferable fallbacks if that route survives.

AMs 1556, 1559 and 1577 take the same approach by deleting core components of Article 88c. If the ordinary legitimate-interest test fits the concrete processing, AI developers can use it. The fact that processing is useful for AI should not change the legal standard.

The expansion amendments show why the dedicated article is risky. AMs 1561, 1563, 1564, 1567 and 1568 expressly extend or restate the route for interests pursued by third parties, with AMs 1561 and 1564 also naming general-purpose AI models. AM 1567 removes the caveat for Union or national laws that require consent, while AM 1568 retains it.

Public-authority processing deserves caution: AMs 1561 and 1562 expressly add an Article 6(1)(e) route for AI processing by public authorities. AM 1592 merely reminds controllers that they must choose the appropriate Article 6 ground, including Article 6(1)(e) for public authorities, and is therefore much less problematic. Article 6(1)(e) already exists and requires a task in the public interest or exercise of official authority grounded in law. An AI-specific restatement can be read as a legislative endorsement of further public-sector reuse when the real question should remain whether the particular processing is necessary, proportionate and covered by the legal task. Something similar happens with the inclusion of third-party interests, which are already part of Article 6(1)(f): naming them again inside an

AI article adds political signalling without solving a legal gap.

AM 1595 demonstrates how far a 'legitimate interest catalogue' can travel. It includes categories such as workplace safety/security, CCTV, IT and business productivity, research and the development of new technologies including AI. Such catalogues risk converting what should be a contextual three-step test into a list of politically blessed interests. The GDPR already allows legitimate interests to be argued for; the law does not need to pre-score them.

An 'unconditional' right to object

The right to object is the alleged counterweight to the new privilege. The Commission proposal contains an unconditional objection safeguard because Article 88c creates a privileged AI route that can be very difficult to contest once data have entered a training pipeline. If Parliament refuses to delete Article 88c, weakening that counterweight makes the architecture worse: AMs 1584 and 1587 delete or reduce it, while AM 1589 replaces it with the ordinary Article 21 model. AM 1574 tries to make objection more usable by allowing a public body to receive objections and send controllers the objection together with pseudonymous identification data. The objective seems attractive, but the design raises new governance problems: a central public body could become a concentration point for identifiers and a registry of people's objections, creating security, purpose-limitation, competence and oversight questions. A decentralised, interoperable relay or privacy-signal architecture could deliver the same usability benefit with less data concentration.

4. Scientific research: genuine research or a general data-reuse route?

Articles 4(38), 5(1)(b), 13(5), 89(1) GDPR + Omnibus Recitals 28, 29 and 32
Simplification verdict: clearer research safeguards could make the existing rules easier to apply. Automatically declaring research reuse compatible, or allowing controllers to skip information duties, goes further: it expands what data can be reused without the ordinary checks

959-960 Delete the new definition of scientific research.

961, 965, 967-968 Requires methodical/systematic, ethical, verifiable or autonomous research with a genuine knowledge or public-interest objective.

962 Excludes profiling, direct marketing, monitoring and influencing/nudging people from research privileges, even if it still enacts the Commission's new broad statutory definition of scientific research, including innovation and commercial interests.

990, 992, 996 Restore the current purpose-limitation approach by deleting the Commission change or returning to the GDPR's existing formulation.

1116-1121 Delete the new Article 13(5) transparency exemption for direct-collection research.

1122 as fallback. Excludes commercial product development, ads, marketing, profiling and commercial model training from the information exemption (which shouldn't exist).

963 Expressly includes AI development, training, testing and validation within scientific research.

964 Adds applied/private research and AI testing/development before market to the privileged definition.

991 Treats further processing for new technical solutions/AI on aggregated data as compatible independently of Article 6(4).

993 Retains the rule that research reuse 'shall be considered compatible' independently of Article 6(4). Adding Article 89 safeguards and lawfulness does not restore current purpose limitation.

1123, 1125 Preserve or broaden the research transparency exemption, including commercial research or purpose changes.

Why this matters

The GDPR, even if not defining the term, already acknowledges the importance of genuine scientific research by giving it significant flexibility, albeit it couples that flexibility with safeguards. The Omnibus changes three things at once: what counts as 'scientific research'; when data collected for one purpose can be reused for research; and when the controller can avoid telling people about that new use. The risk comes from the combination, for a broad definition plus privileged reuse plus weaker transparency will turn 'research' into a general route for commercial data reuse. Article 89 GDPR already deals with what is allowed or not but even more so with what measures need to be taken for something to qualify as science or other under 89(1), and any science-related change should belong, if at all, in this provision.

The future proposed definition of 'scientific research' could also broaden the practical reach of Article 89(2), which allows Union or Member State law to derogate from the rights in Articles 15, 16, 18 and 21 for scientific research, subject to safeguards, necessity

and the requirement that exercising those rights would render the research impossible or seriously impair it. Many Member States have already adopted such derogations on the basis of the existing understanding of scientific research. If the Omnibus now expands that concept to cover a wider range of activities, those existing national derogations could apply to processing activities that national legislators may never have intended to privilege in this way. The result could therefore be a *de facto* expansion of restrictions on access, rectification, restriction and objection without any corresponding reassessment of whether those limitations remain necessary and proportionate for the newly covered activities.

A line to draw.

It is important to stress that commercial involvement is not automatically the problem and does not make research non-scientific. Universities work with companies, and applied research can be commercially funded. The dividing line should be whether there is recognisable scientific inquiry - a method, a genuine knowledge objective, verifiability and appropriate safeguards - rather than routine product optimisation, advertising, profiling or model training being relabelled after the fact.

What do the amendments say?

The LIBE/ITRE draft report (AMs 2, 3 and 45) largely retains the Commission's privileged treatment of scientific research. AM 45 keeps the rule that further processing for research is compatible with the original purpose independently of the ordinary Article 6(4) assessment, while AMs 2 and 3 add recital-level references to the safeguards that must accompany research under Article 89(1) and to the possibility of relying on legitimate interests. Even if slightly better than the Commission's proposal, these do not restore the ordinary purpose-compatibility test.

AMs 959-960 avoid the problem entirely by deleting the new definition. A broad definition introduced through an Omnibus can create incentives for controllers to redesign ordinary development work as research in order to obtain additional flexibility.

If a definition survives, AMs 961, 965, 967 and 968 would offer more defensible criteria. Their wording differs, but the common direction is to require recognisable scientific method, autonomy or independence, verifiability and a genuine contribution to knowledge. AM 962 adds an especially useful negative safeguard by excluding profiling, direct marketing, monitoring and behavioural influence. Those would be the kind of concrete exclusions that **prevent a research exception from swallowing ordinary commercial surveillance.**

AM 970 sits between those camps: it replaces the Commission's loose innovation language with 'creative and systematic work' undertaken to increase the stock of knowledge and expressly covers basic and applied research, but still says research may further a commercial interest, however. That is not inherently dangerous, but it makes it even more important to distinguish genuine research conducted in a commercial setting from

commercial development that simply adopts the research label.

The opposite direction is visible in AMs 963 and 964. AM 963 explicitly say that AI development, training, testing and validation may constitute scientific research. AM 964 similarly opens the definition to private/applied research and pre-market AI work. **The danger is not that AI research can never be scientific, because it plainly can. The danger is that naming AI development as a privileged category invites ordinary model training or product work to claim research status without first demonstrating the characteristics that make the activity scientific.**

A definition that is more dangerous when paired with reuse and transparency privileges

As mentioned, the problem is not just the proposed definition, but the fact that it is coupled with an exemption from purpose limitation, that is, **a shortcut for reusing data**. A broad definition does not operate on its own: it can determine who benefits from a shortcut around the ordinary purpose-compatibility assessment and, through Article 13(5), who may avoid individual transparency duties. In other words, the same wording that might be tolerable as a descriptive definition can become much more dangerous when it automatically unlocks reuse and information exceptions. . The preferred option would therefore be AM 990, which removes the Commission's attempt to make research further processing compatible independently of Article 6(4). AMs 992 keeps the ordinary compatibility assessment and makes clear that ordinary product development or general AI training does not become research simply because a controller uses that label. AM 996 returns towards the GDPR's current, more cautious wording. On the other hand, AMs 994, 995 and 997 remove the Commission's explicit statement that research reuse is compatible independently of Article 6(4), which might look like an improvement. However, they do not fully return to the GDPR's current wording: the GDPR says that qualifying research reuse 'shall not be considered incompatible' with the original purpose. These amendments instead say that it 'shall be considered compatible.' That difference is important because the latter wording comes much closer to deciding compatibility in advance, rather than preserving the ordinary contextual assessment.

By contrast, AM 991 says further processing for new technical solutions, including AI, on aggregated data is compatible independently of Article 6(4). Aggregation may reduce risk, but aggregation is not anonymisation and it should not be a substitute for asking whether a new purpose is compatible and lawful.

Transparency is the third leg of the scientific research three-body problem: a controller should not be able to create the difficulty of informing people through its own architecture and then use that difficulty as the reason not to inform them. AMs 1116-1121 delete the new Article 13(5) exemption that would allow controllers collecting data directly from people to avoid individual information in some research contexts. AM 1122 could be a useful fallback if an exemption remains: it narrows the route and explicitly excludes commercial product development, advertising, marketing, profiling and commercial model training.

5. ‘Sensitive’ data and biometrics: AI should adapt to Article 9, not the reverse

Articles 9(2)(k), 9(2)(l) and 9(5) GDPR + Omnibus Recitals 33 and 34
Simplification verdict: creating new AI or biometric exceptions changes when especially sensitive data may lawfully be processed and is not simplification. Stronger amendments with narrower necessity, one-to-one verification, user-control or deletion safeguards can reduce the damage, but they still leave protection below the GDPR today.

+

1018-1023 Delete the new AI-specific Article 9(2)(k) derogation.

1028-1029 Delete the new biometric-verification derogation in Article 9(2)(l).

1026, 1061 Fallbacks insisting that sensitive data are genuinely incidental/residual and preserving removal/output protections.

1030, 1034–1035 Fallbacks limiting biometrics to one-to-one verification, strict necessity, user control and, where possible, on-device processing/deletion.

−

1024 Turns the AI exception into a wider ‘innovative system or technology’ route and adds third-party interests.

1025 Expands the new derogation across training, testing, deployment, operation, improvement and related products/services.

1027 Explicitly extends the AI special-category route to general-purpose AI.

1033, 1036 Mixed: broaden the proposed biometric exception beyond strict one-to-one verification towards identification or unique-identification uses, but they also make biometric use optional and require a non-biometric alternative.

1039, 1042-1043 Create new public-benefit, contractual, fraud/security or other Article 9 exceptions.

1045 + 1070 Limit Article 9 protection around data that ‘directly’ or intentionally reveal sensitive traits, resulting in a weaker protection for inference.

1056-1059 Weaken removal/output safeguards through risk, feasibility or capability tests.

1072-1073 Create broad public-benefit/'privileged processing' routes, including group administration and employee data.

Why this matters – special categories of data and datasets

Article 9 of GDPR starts from a strict rule: processing data revealing health, ethnicity, political views, religion, trade-union membership, sexual orientation and other specially protected characteristics is prohibited unless a specific exception applies. The Omnibus would add an AI-specific route for special-category data that appear incidentally or residually in AI development or operation. Where removing them would require manifestly disproportionate effort, the data may remain, subject to safeguards. That changes the starting question from 'is there a narrow legal reason to process these data?' towards 'the data are already in the system… how hard would it be to remove them?'.

Large AI datasets can contain sensitive information accidentally or at scale. That is a real engineering problem, but **technical inconvenience is not itself a GDPR legal ground.** Otherwise the largest and least curated datasets would obtain the broadest exception because they are the hardest to control.

Legal Concepts - Article 9 starts from a prohibition

Health data, data revealing racial or ethnic origin, political opinions, religion, trade-union membership, sexual orientation and other special categories receive additional protection. Article 9 starts from a prohibition and then lists specific derogations. A new derogation is therefore not just guidance about risk mitigation; it expands the circumstances in which such data may be processed.

What do amendments say?

The LIBE/ITRE draft report takes two different approaches to special-category data. First, it leaves the Commission's new AI-specific derogation in Article 9(2)(k), Article 9(5) and Recital 33 essentially untouched. Second, on biometrics it does intervene: draft-report AMs 4 and 46 keep a new biometric-verification derogation but narrow it towards one-to-one verification, necessity and proportionality, safeguards under Union law and a stronger concept of 'sole control.' The draft report is therefore passive on the AI exception but damage-limiting on biometrics. Neither approach restores the current Article 9 baseline, but they should not be described as the same thing.

AMs 1018-1023 provide the strongest answer: delete the technology-specific exception and require AI processing to fit the existing Article 9 structure. This preserves technological neutrality and avoids creating a precedent whereby scale or technical inconvenience becomes a reason to invent a new exception to a prohibition designed to protect especially sensitive information (related Recital 33 AMs 296–310).

If the new Article 9(2)(k) survives, AMs 1026 and 1061 are better fallback territory. AM 1026 tightens the concept further. AM 1061 preserves an obligation to remove the data where

possible and, where removal would be manifestly disproportionate, to prevent further processing, outputs and disclosure. AM 1025 appears positive at first because it insists that the sensitive-data presence be incidental and residual, but it also applies the route across a broad AI lifecycle and contributes to legal uncertainty.

AM 1024 illustrates perfectly well why the category is dangerous once created: it would extend the logic from AI to innovative systems or technologies more generally, **demonstrating how a supposedly narrow technical problem can become a general innovation derogation.** AM 1027 similarly singles out GPAI.

Several amendments create new Article 9 exceptions unrelated to the Commission's AI rationale. AM 1040 covers the administration of retirement, disability and dependency benefits: it is comparatively narrow and contains safeguards, but the first question should still be whether existing Article 9 grounds already cover the legitimate use cases. AM 1043 is much broader: fraud, abuse, automated traffic, identity misuse, account takeover and payment security can justify extensive profiling and inference. Security measures should constrain otherwise lawful processing and should not become a general-purpose sensitive-data gateway.

The inferred-data amendments are particularly serious. AM 1045 and the related AM 1070 focus Article 9 on information that 'directly' or intentionally reveals a sensitive trait. That risks downgrading the protection of inferences: a system may infer religion, health, political views or trade-union membership from apparently ordinary data even if the input field does not directly announce that fact. The harm does not disappear because the sensitive characteristic was inferred rather than explicitly supplied.

Why this matters – the added sensitivity of biometrics

The biometric amendment deserves a separate explanation. Verification asks 'are you the person linked to this credential?' – for example unlocking your own phone with your fingerprint. Identification asks 'which person in this group is this?,' such as matching a face against a watchlist. **Moving from one-to-one verification to one-to-many identification is a qualitatively different surveillance risk.**

The LIBE/ITRE draft report (AMs 4 and 46) keeps the Commission's new biometric-verification derogation, even if it narrows and safeguards it by specifying one-to-one verification, adding necessity and proportionality, requiring appropriate safeguards under Union law and strengthening the meaning of 'sole control,' including limits on the controller's ability to access biometric data in decrypted form.

AMs 1028-1029 delete the new exception entirely (related Recital 34 AMs 4 and 311–322). If Parliament insists on retaining text instead of rightfully rejecting the new biometric Article 9 exception, AMs 1030, 1034 and 1035 contain potentially useful limiting ideas: one-to-one verification rather than identification, strict necessity, user control, on-device processing where possible and deletion.

AMs 1033 and 1036 need a mixed assessment. Both are problematic because they broaden the proposed exception beyond strict one-to-one verification: AM 1033 covers verification

or identification, while AM 1036 permits processing for uniquely identifying a person. That creates a qualitatively different surveillance risk. At the same time, both add a meaningful safeguard that the current paragraph should acknowledge. They make biometric use optional and require a non-biometric alternative of comparable effectiveness, with AM 1033 also protecting people who do not consent from image capture. That raises a further question: if the biometric route is genuinely optional and based on a free choice, why is a new Article 9 derogation needed at all rather than relying on explicit consent under Article 9(2)(a), where consent is actually valid? Their voluntary-use safeguard is worth preserving, but it does not justify a broader statutory exception.

6. Automated decisions: efficiency is not the same thing as necessity

Article 22 GDPR + Omnibus Recital 38
Simplification verdict: clearer rules on necessity and meaningful human review can reduce uncertainty; redefining necessity around business convenience makes the substantive protection weaker. Simplification should make the existing test easier to apply, not make more significant decisions automatable.

+

51 and 53 (Draft Report) Keep the current prohibition-with-exceptions logic, and strengthens the requirement of meaningful human review

362 Recital says efficiency, cost, scalability, speed or business-model choices are not enough to establish contractual necessity.

368 Recital interprets significant effects broadly and strengthens the conditions around solely automated decisions.

−

1146 Preserves the weakened necessity logic and focuses only on less intrusive automated alternatives.

1154 Creates an exception where an AI decision can be reviewed by a human before or after, risking post-hoc rubber-stamping.

1141-1145 Delete/rewrite the Commission Article 22 approach and restore a rights-based framing.

1147-1151 Remove the 'regardless of human alternative' language and restore stricter necessity.

1153, 1155 Requires meaningful human intervention by a competent reviewer with power to change the result.

1161 Examines data, logic and consequences, gives override authority and protects reviewers from retaliation.

1166 Adds a DPIA trigger for large-scale consequential automated decision-making.

Why this matters

Article 22 is the GDPR safeguard for decisions based on automated processing that produce legal or similarly significant effects (for example decisions about credit, insurance, employment or access to an important service). **The current provision is framed as a right not to be subject to such decisions, subject to limited exceptions. The Commission's proposal rewrites it from the opposite direction, beginning with circumstances in which solely automated decisions are allowed. Even where lawyers debate how much that reframing changes by itself, it shifts the centre of gravity from a right with exceptions to a permission with conditions.**

The most concerning substantive change, however, concerns the so-called 'necessity test.' One exception covers automated decisions necessary for entering into or performing a contract. The Commission's text would consider that automation can still be necessary even when a human could take the decision, a proposal that collapses necessity into convenience. A company may prefer automation because it is cheaper, faster, more consistent or easier to scale; **the legal and rights-centered question is whether the contractual purpose genuinely requires the significant decision to be taken solely by automated means.**

A practical example

A bank uses an automated system to decide whether someone gets a loan. The system rejects the application, and a human employee could review the case, but the bank prefers automation because it is faster and cheaper. Under the Commission's wording, the bank could still argue that the automated decision is 'necessary' for the contract.

What do the amendments say?

The LIBE/ITRE draft report **(AMs 6, 51, 52 and 53)** makes an important correction. AM 51 restores Article 22's rights-based framing by reinstating the right not to be subject to solely automated decisions with legal or similarly significant effects. AM 52 largely carries over the existing statutory-authorisation exception and is not the substantive change to focus on. The key improvement is AM 53, which strengthens the safeguard of human intervention by requiring a reviewer with the authority, knowledge and competence to change the decision and to assess the relevant data rather than merely the system output. Its wording can be improved further: meaningful review should include enough understanding of the logic and relevant factors to examine why the system produced this particular decision, otherwise a human reviewer can still rubber-stamp an automated result. AM 6, on Recital 38, mirrors that rights-based framing and rejects purely symbolic human involvement. However, this amendment also retains the Commission's controversial proposal that automated decision-making can still be considered 'necessary' for entering into or performing a contract even where a human could take the decision, subject only to choosing the less intrusive option among equally effective automated solutions. In practice, this could allow a company to argue that a fully automated credit, insurance or hiring decision is 'necessary' simply because automation is its chosen way of delivering the service, even though a meaningful human alternative exists.

Many tabled amendments show that Article 22 is one of the provisions with the greatest potential for genuine improvement: several packages go beyond merely restoring the current wording and propose stricter necessity tests, broader interpretations of significant effects, stronger explanation rights and much more substantive human review.

The amendments split between restoring that strict test and preserving or expanding the efficiency rationale. AM 362 is useful because it states the necessity problem in terms controllers and courts can apply: **usefulness, efficiency, economic advantage, scalability, speed, consistency, business-model choice and cost reduction do not by themselves make full automation necessary.** AM 1142 then turns that logic into one of the most complete operative alternatives, while AMs 1147-1151 remove the Commission sentence that would detach necessity from the existence of a human alternative.

AM 1156 is also worth flagging and is one of the best examples of an amendment contributing further to legal uncertainty. It inserts a separate right not to be subject to a solely automated decision producing legal or similarly significant effects (related Recital 38 AMs 360–377). Read on its own, that seems protective because it does not repeat the

Commission's exceptions. Read alongside the rest of Article 22, however, it foregoes the exceptions in current 22(2), and the relationship between that new paragraph and the remaining permission structure is unclear. Parliament should strengthen the right without creating two overlapping rules whose interaction would itself need to be litigated. AM 1146 goes the other way: it preserves the Commission's basic premise and asks only whether a less intrusive automated solution can achieve the same result without disproportionate administrative burden. That is too narrow, because the comparator should not be limited to another automated technique: the question is whether the significant decision really needs to be taken solely by automated means at all.

AM 1146 further dilutes the necessity test for entering into or performance of a contract by requiring the controller to select a less intrusive automated processing solution only when this does not result in a significant additional administrative burden. AM 1154 expressly allows automated decisions taken by an AI system, as long as there is some unspecified human review and oversight.

A human in the loop

The human review amendments are equally important because controllers can otherwise avoid Article 22 by inserting nominal human involvement. AMs 1153 and 1155 require a reviewer who actually understands the case and can change the result. AM 1161 goes further: the reviewer must examine the relevant data, logic and consequences, have the competence and authority to override the system, and be protected against retaliation for doing so. This is particularly valuable in employment settings, where a reviewer who is formally empowered but practically punished for disagreeing with an algorithm is not meaningful oversight.

AM 1154 should be rejected because it risks turning the mere availability of a human review before or after the decision into a legal exception. Post-hoc appeal rights can be important safeguards, but they do not necessarily change the fact that the original significant decision was made solely by automated means.

AM 1152, which removes explicit consent as a basis for certain solely automated decisions involving children, has a strong substantive objective. However, its implementation would need care. If the legal permission changes according to whether an individual is under 18, services may respond by age-assuring everyone. A safer drafting approach should protect known, suspected or reasonably foreseeable child users from automated decisions while also specifying that this does not create a legal basis or obligation to verify people's age.

7. Access and information: rights should not depend on why a person asks

Articles 12(5) and 15, 13(4) and 13(5) GDPR + Omnibus Recitals 35, 36 and 37 Simplification verdict: common formats and clearer procedures could make rights easier to exercise. New motive tests, refusal grounds or transparency exemptions do the opposite: they narrow the entitlement itself or make people work harder to obtain information. That is deregulation and not administrative simplification

+

5, 48 and 49 (Draft Report) Delete idea of access abuse

329 Recital recognises access as enabling employment, non-discrimination, defence, consumer and collective-redress rights.

1080 Removes the idea that using access for purposes beyond data protection is abusive; retains manifestly unfounded/excessive limits.

1088 Clarifies that good-faith compliance checks, including Article 80 assistance, are not automatically unfounded/excessive. 'Good faith,' however, must not become a new condition for access or a licence to investigate motives

1093-1094 Keeps the burden on the controller and recognises legitimate purposes such as employment, consumer, equality, journalism and collective redress.

1116-1121 Delete the new Article 13(5) research-information exemption.

1134 Adds the legal basis to the information available through access.

−

1089-1092 Delete or weaken the controller's burden to demonstrate that a request is manifestly unfounded/excessive.

1095 Allows the controller to ask the person to specify scope and reasons for the request.

1096 Gives the Commission power to define abuse/excessiveness through implementing measures.

1196, 1109 Broaden information exemptions or weaken active information duties through impossibility, disproportionate effort, resources or 'reasonable steps'

1114 Restricts copies and excludes requests made exclusively for disputes, pre-litigation or judicial proceedings.

1127, 1132 Deem Article 14/13 information fulfilled through accessible website publication.

1129, 1133, 1137 Narrow what must be provided as a copy or broaden controller interests/ disproportionate-effort arguments.

Why this matters

The online realm is structurally asymmetric. An organisation normally knows what data it holds, where the data came from, which systems use them and who receives them; the person usually does not. GDPR transparency and access rights exist partly to correct that imbalance: **without visibility, rights to rectification, erasure, objection, non-discrimination or effective remedy can become largely theoretical, if not outright practically impossible.**

Access Rights

The Omnibus proposal changes two different mechanisms. Access under Article 15 is reactive: a person asks an organisation what personal data it processes and receives a copy plus information about the processing. **The proposal to change Article 12 would add a new 'abuse' concept linked to using access for purposes other than data protection, lower the controller's burden for treating a request as excessive and encourage people to be as specific as possible.**

Genuinely abusive conduct does not require a broad new motive test. Article 12(5) already permits refusal or a fee for manifestly unfounded or excessive requests, and the general EU law doctrine of abuse applies exceptionally. In Brillen Rottler (C-526/24, 19 March 2026), the CJEU confirmed that even a first access request may exceptionally be refused as excessive where the controller proves abusive intent, for example where the request is made solely to artificially create the conditions for obtaining an advantage under the GDPR. **The Court stressed that Article 12(5) is an exception, must be interpreted restrictively and places the burden on the controller. That is very different from treating ordinary ulterior purposes, such as employment litigation, journalism, consumer claims or collective redress, as abusive.**

The LIBE/ITRE draft report (AMs 5, 48 and 49) significantly improves the Commission proposal on access by deleting the new idea that Article 15 can be abused merely because a person uses access for purposes beyond data protection, restores the controller's full burden of proving that a request is manifestly unfounded or excessive, and explicitly recognises that data protection rights may legitimately enable other rights or public-interest aims.

AMs 1080, 1093 and 1094 respond to an increasingly important misconception: a person does not lose the GDPR right of access because they hope to use the information for employment litigation, a consumer claim, anti-discrimination proceedings, journalism or collective action (related Recital 35 AMs 323–334). Article 15 is a data protection right, but people can legitimately use the information they obtain to exercise other rights. AM 1088 tries to protect people who use GDPR rights in good faith to check whether a controller is complying with the law, including with the help of an Article 80 organisation. That objective is useful, but the wording is risky, because referring specifically to 'good faith' can suggest that controllers may investigate whether other requests were made for the right motives. Access rights should not depend on proving an approved purpose or state of mind. The safer approach is to make clear that compliance checks are protected without turning good faith into a new condition for exercising the right.

AM 329 is a useful recital amendment because it makes the enabling function explicit: access may support employment rights, non-discrimination, rights of defence and collective redress. This does not turn Article 15 into unlimited discovery but clarifies why the existence of another legal dispute does not automatically make the data protection request abusive.

AM 1114 is therefore particularly dangerous. It restricts the copy right and creates an exclusion for requests made exclusively in the context of a dispute, pre-litigation or court proceedings. That would hit precisely the situations in which information asymmetry is most acute. **It also invites controllers to litigate about the person's motive before responding to the underlying access request - the opposite of simplification.**

Information Rights

On the other hand, information duties under Articles 13 and 14 are proactive: the controller must tell people what it is doing when data are collected from them or obtained elsewhere. The proposal broadens circumstances in which that individual information can be skipped. This is not limited to the new research-related exemption mentioned above. Article 13(4) would also allow controllers to withhold parts of the information where data are collected in a 'clear and circumscribed' relationship, the activity is not data-intensive and there are reasonable grounds to assume that the person already has certain information. This is where the information asymmetry becomes decisive. Requiring a person to make a very specific request can demand that they already know what data are held, which processing operation matters and sometimes which entity in a complex chain has them.

The LIBE/ITRE draft report does not amend the Commission's proposed changes to Articles 13(4) and 13(5), nor the related Recitals 36 and 37.

AMs 1116-1121 delete the new research exemption for data collected directly from the person. That deletion is important because the Commission proposal would create a new route for controllers to avoid giving individual information about later research processing where providing that information would involve disproportionate effort. Removing Article 13(5) keeps the ordinary Article 13 rule: when the controller collected the data from the person, the controller normally has to tell that person how the data will be used.

AM 1132 goes much further in the opposite direction by deeming Article 13 fulfilled if the information is published and maintained accessibly on the entity's website; AM 1127 does the same for Article 14 which is even more problematic because the data subject is generally not even aware of the processing when the personal data is not collected from them. Article 14(5)(b) has a narrow exception to replace the individual notification with a general notice published on a website when the individual notification would involve a disproportionate effort. **Turning this into a general exception from the individual right to information, as AM 1132 does, would undermine the purpose of Article 14 and the exercise of other data subject rights because they are preconditioned on having been informed about the processing.**

AMs 1129, 1133 and 1137 narrow access and the copy right in different ways, and none should be treated as simple housekeeping. **AM 1129** excludes data that the person created, authored, transmitted or received and that remain available through the controller's system or by other lawful means. If the data are genuinely easy to access already, the controller

can point the person to them in responding to the request. A categorical exclusion is unnecessary and can prevent the person from verifying what exact data the controller actually processes, stores or passes downstream. **AM 1133** confines the copy to the 'personal data as such,' which risks excluding contextual material where context is needed to make the data intelligible. **AM 1137** is particularly dangerous. It expressly expands the existing protection for the 'rights and freedoms of others' to include the controller itself and adds impossibility or disproportionate effort as grounds for withholding the copy. That gives the party subject to the access duty a new interest to balance against the person exercising the right. Trade secrets and other legitimate interests can already be protected without turning the controller's own interests into a general route for narrowing access.

8. Keep terminal-equipment confidentiality in ePrivacy

Proposed Article 88a GDPR, Article 5(3) ePrivacy Directive + Omnibus Recitals 43-47

Simplification verdict: device confidentiality is a fundamental-rights safeguard, not a data-classification exercise. Moving part of that protection into the GDPR muddles rules over access to a person's private device with assessment of whether the information involved qualifies as personal data. The stronger and clearer approach is to keep one confidentiality rule in ePrivacy, protecting the device regardless of the type of data involved, with the GDPR governing subsequent processing of personal data

+

1365-1366, 1365–1366 Delete proposed GDPR Article 88a while expressly moving the device-access rule back to ePrivacy.
While the best option is for Parliament to remove article 88a entirely, the following amendments would provide some damage limitation:

1373 Prohibits denying service/functionality merely because a person refuses non-strictly-necessary access.

−

1370 Treats terminal-access consent as also covering subsequent processing necessary for the consented purpose.

1385, 1406 Creates a consent-free contextual-advertising route. –

1403-1404, 1406 Create a narrower contextual-advertising route but still turn a preferred advertising model into a permission to access the device.

1376 Protects anonymity/encryption where law-based terminal access is used.

1380 Clarifies that Article 88a cannot justify communications-content access, weakening E2EE, client-side scanning or covert/fingerprinting practices.

1382 Adds 'strictly' to the requested-service necessity test.

1389 Deletes the audience-measurement exception.

1391-1392 Fallback: limit measurement to anonymous/aggregated, own-use, non-tracking forms.

1400 Narrows security access to demonstrably necessary/proportionate technical security.

1414, 1416-1417 Require consent for behavioural/profile uses, preserve ePrivacy and prevent one user consenting to access data about other people on their device.

1713 Extends confidentiality protection explicitly to data related to/processed by terminal equipment.

1714-1716, 1724 Delete the Commission carve-out from Article 5(3) ePrivacy.

1725, 1728 Rights-protective ePrivacy replacement approaches with tighter technical/anonymous exceptions.

1394-1397, 1412 Expand consent-free audience measurement to third parties/EMFA contexts.

1398 Broad security/anti-abuse exception extending even to uses contrary to provider terms and conditions.

1405, 1408, 1410-1411, 1413 Use legitimate interest and/or PETs as a consent-free route to terminal access.

1426, 1437, 1441 Create media exemptions from refusal/no-reprompt rules or explicitly enable media consent-or-pay.

1594 Rebuilds strong communications-confidentiality and terminal-equipment rules inside the GDPR. Even if its substance is considerably stronger than the Commission proposal, relocating ePrivacy protection into the GDPR creates structural and competence risks.

1727 Keeps ePrivacy as the legal home but allows broad functionality/personalisation/audience-measurement exceptions.

1730 Moves personal-data processing previously covered by ePrivacy exclusively into the GDPR.

Why this matters

ePrivacy protects the confidentiality of information stored in or accessed from phones, computers and other user equipment. That protection is attached to the act of accessing, reading or modifying a private device, regardless if the information happens to qualify as personal data. **It protects the fundamental right to privacy. The GDPR, protecting another fundamental right (to data protection), asks a different question: once personal data are**

being processed, on what legal basis and subject to which safeguards?

The current position is clear: Article 5(3) of the ePrivacy Directive requires user consent before storing or accessing information on a user's device (e.g. through cookies or device fingerprinting), except in certain specific narrow circumstances, regardless of the nature of the data concerned. The Commission would split the current rule. Where device access concerns personal data or 'leads to' (an expression that has no clear ex ante boundary and makes it difficult for users, controllers and authorities to know which regime applies at the moment of access.) personal data processing, new GDPR Articles 88a/88b would apply; Article 5(3) ePrivacy would remain for other information.

That creates complexity by adding an additional threshold question whereas the Omnibus is supposed to make the rules the simplest possible: before deciding whether someone may enter the device, parties may have to argue about whether what will be read or written constitutes (or will 'lead to') personal data processing. The problem is not merely simplicity, because the rules protect overlapping but different fundamental rights. **A single device-access/confidentiality rule in ePrivacy gives the device the same lock regardless of the legal status of the information behind it. If the information is personal data, the GDPR then governs what happens next.**

What do the amendments do?

The LIBE/ITRE draft report does not substantially alter the Commission's proposed restructuring of terminal-equipment confidentiality. Its amendments (AMs 43-44) are essentially technical definitions, rather than changes to the substantive relationship between the GDPR and Article 5(3) ePrivacy.

The strongest approach to simplification here is to remove Article 88a, as proposed by AMs 1365-1366, keeping device access rules properly within ePrivacy. Alternatively, there may be opportunities to make improvements to operation of Article 5(3). For example, AM 1725 keeps the lock on the device in ePrivacy and allows tightly framed technical exceptions, including immediately anonymised and aggregated audience measurement. AM 1728 also preserves ePrivacy with narrow exceptions and easy refusal/no-reprompt logic. AM 1727, shows the opposite problem. It keeps ePrivacy as the legal home, but paragraph 2 creates broad consent-free routes for full functionality, personalisation, recommendations and several forms of audience measurement, while paragraph 4 expressly allows media services to condition access on consent to processing for purposes including advertising, product development and analytics or on payment for an equivalent version. **Keeping the right instrument is necessary, but the exceptions must remain narrow enough that the rule still has content.**

Moving ePrivacy into the GDPR

A package of amendments around AM 1594 try to rebuild strong communications-confidentiality protections inside the GDPR. Their defensive motivation is understandable, especially in a broader Brussels debate about whether ePrivacy should survive as a separate instrument. But the strategy is risky. ePrivacy and the GDPR protect overlapping

but distinct, interests and fundamental rights: ePrivacy protects the confidentiality of communications and the private sphere of a device, while the GDPR regulates the processing of personal data. Moving the former into the latter risks turning a simple confidentiality rule - do not access or store information on someone's device unless a narrow exception applies - into a question that depends on whether the information is personal data and which GDPR legal basis or exception can be invoked. It may also politically make ePrivacy easier to abolish later on the ground that its protections have already been 'absorbed.' It's critical to bear in mind that a strong rule in the wrong legal architecture can still weaken protection in the long term.

If Parliament keeps Article 88a despite its structural shortcomings, or if its essence is moved to Article 5(3) ePrivacy Directive, some amendments can still reduce the damage. AMs 1382, 1391-1392 and 1400 tighten the service, audience-measurement and security exceptions. AMs 1407 and 1414 add anti-circumvention limits so that exceptions cannot become routes for tracking, profiling, behavioural advertising or sensitive inference.

Amendments focussed on contextual advertising illustrate the same point. Genuine contextual advertising is selected from the page or content being viewed rather than a person's past behaviour. That is less intrusive than behavioural advertising, but must not be used to provide a back-door into legitimising harmful tracking practices. AMs 1385, 1403-1404 and 1406 risk turning a preferable business model into a new legal permission, given that they create consent-free device access for advertising measurement or related functions under a broad 'contextual' label. Ad selection should be based only on the immediate non-personal content rather than the use of search queries, persistent identifiers, cross-service linkage or other personal data. While mechanisms to encourage industry uptake of contextual advertising should be considered, the Omnibus is not the right vehicle for this. AM 1594 contains some valuable ideas (and would make for a better position than the Commission's proposal), but it is premised on the problematic movement of device confidentiality into GDPR, and pre-empts a broader policy debate.

Security is another area where gaps can expand too quickly. A narrow exception for maintaining technical security can be justified, and this is something that the Parliament already did when setting a position for the ePrivacy Regulation. However, an exception that covers fraud, non-human traffic, misuse, circumvention and violations of a provider's terms and conditions risks turning a company's private contractual rules into a statutory permission to enter a person's device. AM 1398 is the clearest example: it broadens the Commission's security exception to cover not only security and integrity, but also the 'functioning' of a service, fraud, automated or non-human traffic, misuse, circumvention of access conditions and even conduct contrary to a provider's terms and conditions. AM 1401 also expands the exception to fraud prevention and technical incidents, while AM 1399 is narrower and at least adds a fundamental rights balancing condition. AM 1400 goes in the opposite direction, limiting the exception to demonstrably necessary and proportionate technical security. A narrow security exception can be justified; an exception that reaches contractual rule-enforcement risks turning a company's private terms into a statutory permission to enter a person's device.

PET-based exceptions such as AMs 1405, 1408, 1410-1411 and 1413 make the same conceptual mistake as the anonymisation debate mentioned above. PETs can make otherwise lawful

access less intrusive; they do not answer the prior question whether access to terminal equipment is legally permitted and justified. If privacy technology itself becomes the permission, the law starts rewarding controllers for mitigating an intrusion that it has not first established they were entitled to make.

Finally, several media-related amendments weaken the user-facing safeguards around device access. AM 1426 exempts media from one-click refusal; AM 1437 exempts them from the six-month no-reprompt rule; AM 1441 even expressly enables deeply troubling media consent-or-pay models. Sustainable journalism is a real policy challenge, but privacy rights do not vary according to the business sector of the service people visit.

It is vital to understand that **cookie banners are deeply inconvenient, but they are a symptom and not the underlying problem.** They proliferated because large parts of the online economy chose to depend on invasive tracking to get our data, and then repeatedly ask people for permission to do it. The solution some industry actors are proposing now is to legalise more device access without consent, which would mean even more tracking. There is another rights-respecting alternative, though: make people's choices easier to express and harder to ignore. Binding privacy signals (more on it just below) can remove much of the repeated prompting while preserving the fundamental right to confidentiality of communications and devices. Broader exemptions, however, do the opposite: they remove the prompt by removing the protection.

legal concepts - ePrivacy protects the device before the GDPR asks what happens to personal data

Article 5(3) ePrivacy protects information stored in or accessed from a person's terminal equipment. The legal logic is tied to the act of entering the private sphere of the device, not only to whether the information qualifies as personal data. If the information is personal data, the GDPR then governs the subsequent processing.

9. Privacy signals: the clearest test of whether simplification is real and rights-respecting

Proposed Article 88b GDPR + Omnibus Recitals 45 and 46
Simplification verdict: a durable, binding privacy signal can remove repeated banners while preserving choice. This is one of the clearest opportunities for genuine rights-respecting simplification.

+

1458, 1465, 1469, 1478 Package around informed choices, controller-/purpose-specific consent and withdrawal.

1457, 1464, 1470, 1476, 1482, 1493, 1498 Strengthen legal effect, refusal/objection/withdrawal and anti-reprompt safeguards.

1463, 1471, 1477, 1483–1485, 1492, 1495 Preserve refusal and objection, allow authorised agents and limit repeated prompting.

1496–1503 Delete the media exemption from signal obligations; legal effect is useful even where some sponsors' wider packages are anti-signal.

1516 Requires open, royalty-free/interoperable specifications and rejects the idea that technical conformity alone proves lawful processing.

1518 Deletes the presumption of conformity from standards.

1534–1535, 1538–1541 Support browser/OS/app functionality, independent privacy agents, DMA-gatekeeper interoperability and full-stack non-discrimination.

−

1443–1455 Form part of packages that delete or hollow out Article 88b.

1459–1468 Delete automated consent or the paragraph making machine-readable choices available.

1473–1475 Delete automated refusal/objection.

1488–1491 Delete the controller duty to respect signals.

1504–1505 Preserve or broaden media exemptions.

1506 Says controller-specific consent prevails over a conflicting automated signal without stating that consent must be the later choice.

1536 Replaces a concrete browser duty with 'market-driven solutions' and preserves more room for service-level overrides.

1544 Removes the long implementation delay.

Why this matters

So-called 'cookie-banner fatigue' is one of the few problems in the Omnibus debate that almost everyone understands. And one of the few things the Omnibus gets right: **binding machine-readable privacy signal offer a direct and rights-respecting solution: people can express a durable choice through their browser, operating system, app or an independent privacy agent, and controllers can read that choice automatically instead of asking again on every site.** The issue is therefore an **unusually clear test of whether 'simplification' means fewer repetitive interfaces or fewer rights.**

The Commission proposal is therefore valuable in principle: Article 88b would require online interfaces to let people communicate consent, refusal and objection through automated machine-readable means and to respect those choices. But its design also relies heavily on standardisation processes, gives media providers an unjustifiable categorical exemption and gives browser providers a much longer implementation horizon.

The Parliament debate

The LIBE/ITRE draft report does not redesign the Commission's machine-readable privacy-signal system.

The parliamentary debate is an interesting one, because it's not simply 'signals or no signals.' The amendment pattern points to a majority for retaining a signal mechanism in some form, while the real conflict concerns its legal effect, the choices it can carry, who must implement it and how quickly. The full-deletion camp is relatively clear: AMs 1443-1454 delete Article 88b as a whole. A second family keeps the article but weakens it, for example AM 1455 reframes it as voluntary, AMs 1459-1462 delete paragraph 1, AMs 1466-1468 remove specific consent functionality and AMs 1488-1491 delete the controller's duty to respect signals.

A third family strengthens user control and lifecycle coverage: AMs 1469-1472 clarify specific consent choices, AMs 1476 and 1478 broaden refusal, objection and withdrawal, and AMs 1482-1484 add withdrawal and objection expressly. A fourth family concentrates on legal effect and technical governance: AMs 1493-1494 make choices binding or purpose-linked, AMs 1516 and 1518 reduce the risk that standards become a legal safe harbour, and AMs 1534-1535 and 1540-1541 address browsers, operating systems, apps and independent privacy agents.

The first priority is to preserve the legal duty to respect automated choices. The Commission proposal already contains that core obligation in Article 88b(2): controllers must respect

the choices communicated through automated and machine-readable means. That is the part that turns a browser or device signal from a technical preference into something that actually changes behaviour. AMs 1488–1491, which delete that duty, would hollow out the entire mechanism: people could signal 'no,' but websites would remain free to ignore it and keep asking. AM 1493 goes in the opposite direction and makes the signals expressly legally valid, binding and enforceable, while also preventing controllers from simply asking again through another interface for the same purpose. AM 1494 also retains the duty to respect the choice while linking it more clearly to the purposes for which consent or objection is sought. Without a binding effect, automated signals do not solve consent fatigue; they merely add another layer on top of the cookie-banner system.

The content of the choice matters too. Refusal, objection and withdrawal should all be expressible through the same machine-readable mechanism. AM 1478 improves the Commission text by adding withdrawal of consent alongside refusal and objection, while AMs 1482–1484 similarly ensure that withdrawal and objection remain part of the automated-choice architecture. This is important because people should not have to use a browser signal to say 'no,' but then navigate a separate website-specific process if they later want to withdraw consent they previously gave. A system intended to reduce friction should reduce it across the entire lifecycle of the choice, not only at the moment consent is first requested.

Consent and refusal are not, however, perfectly symmetrical. A person may set a broad preference such as 'refuse tracking' and later decide that they do want to consent to one particular controller and one particular purpose. That should remain possible. AM 1481 usefully recognises that a general automated preference should not prevent a person from making a service-specific choice. The wording in AM 1506 is problematic despite sitting inside an otherwise relatively rights-respecting signals package. The package is meant to make automated privacy choices meaningful and binding, but this amendment risks hollowing that out by stating that specific consent prevails over a conflicting automated signal without saying that the consent must be the person's later choice. In practice, an old consent could therefore trump a newer refusal expressed through a browser or operating-system signal, and that could make the signal ineffective precisely where it is supposed to protect the person from repeated prompting.

The media exemption should be removed. AMs 1496-1503 delete the categorical exemption for media service providers and should be supported. AM 1504 keeps an exemption for media meeting specified EMFA conditions and gives certain news and current-affairs services a route into browser or operating-system recommended choices or whitelists. That may respond to a genuine media-sustainability concern, but it still leaves a sectoral carve-out from a user-facing privacy mechanism. AM 1505 broadens the exemption even further. Sustainable journalism matters, but the legal effect of a person's refusal, withdrawal or objection should not depend on the activity of the controller.

The standardisation debate is equally important. Technical standards are useful for deciding how a signal is encoded and transmitted so that browsers, apps, operating systems, websites and other software can understand each other. They should not decide what the law means. The Commission proposal asks standardisation bodies to develop standards for the 'interpretation' of machine-readable choices and gives conforming interfaces a presumption of compliance. That risks shifting substantive questions - what counts

as consent, what a refusal covers, when an objection is binding - from legislation and data protection law into technical standard-setting. AM 1516 offers a much safer model: specifications should be open, royalty-free, interoperable and independently verifiable, and compliance with a standard should not create a presumption that the underlying processing is lawful. AM 1518 likewise removes the Commission's presumption of conformity. AMs 1513–1514 improve governance by bringing in the EDPB, EDPS and other stakeholders, but they still leave considerable weight with standards. The principle should be clear: standards carry the choice; the law defines its legal effect.

Finally, the architecture also matters for competition as well as privacy and data protection. If only the dominant browser or operating-system provider can communicate choices, the EU risks solving one gatekeeping problem by creating another. AM 1535 therefore usefully extends the obligation beyond browsers to applications and operating systems and allows refusal or objection to be configured by default. AM 1534 explicitly requires infrastructure to accommodate authorised third-party software or agents, while AM 1540 goes further for DMA gatekeepers by requiring them to let structurally and economically independent third parties convey users' choices. AM 1541 adds safeguards against preferential treatment and manipulative design. These amendments point towards a more robust model: mandatory interoperability across browsers, operating systems and apps, combined with room for independent third-party agents and no ability for a dominant platform to privilege its own consent-management tool. By contrast, AM 1536's reliance on 'market-driven solutions' is weaker: if the legal obligation depends too heavily on what the market chooses to build, the largest browser and platform providers are likely to shape the architecture themselves.

Last but not least, the implementation timeline should also not become an excuse to postpone the right into irrelevance. AM 1548 shortens the browser obligation to 24 months, while AM 1547 links application to publication of the relevant standards with a 12-month period afterwards. The stronger objective should be to ensure that the legal duty exists from the outset and that technical implementation follows quickly, rather than leaving people with several more years of banners – and potentially, more consent-free tracking - while the market waits for standards to mature.

10. When simplification becomes an excuse to rewrite the GDPR

The amendments tabling has not only produced competing versions of the Commission proposal supposedly containing only 'targeted amendments.' **MEPs have also tabled ideas that were not really part of the original Omnibus at all.** Some respond to real implementation problems and could make the GDPR easier to comply with or enforce without weakening rights. Others use the Omnibus as a vehicle for much more radical rewrites: new scope exemptions based on company size or sector, weaker remedies and enforcement, technology-based safe harbours, pre-approved legitimate interests and a lower benchmark for international transfers. This section discusses these ideas because Parliament may nevertheless have to vote on them, but their inclusion here should not be read as support for addressing these questions through the Omnibus. **Structural reforms to the GDPR and its enforcement architecture require a separate, evidence-based process with full fundamental-rights safeguards, something that the Digital Omnibus direly lacked from the beginning.**

Do not export the Omnibus into law-enforcement data protection

+ AMs 9, 10

− AMs 265, 396, 397, 401, 1005, 1011

The Omnibus is already reopening the GDPR and ePD. **It should not also become an instruction to reopen the Law Enforcement Directive (LED), where the legal context, purposes and safeguards are different.** The joint draft report moves in the right direction: draft-report AMs 9 and 10 remove language that would have politically pre-committed the EU to aligning the LED with whatever changes are eventually made to the GDPR.

Several tabled amendments push the opposite way. AMs 396, 397 and 401 keep or strengthen the idea of future LED alignment, with AMs 396 and 401 adding a one-sided guarantee that alignment must not impair law-enforcement processing. AM 265, and the related operative AMs 1005 and 1011, should be treated separately from the ordinary GDPR scope exclusion: processing in the course of an activity that falls outside Union law is already excluded by Article 2(2)(a). Where a public authority is subject to the GDPR, national-security-related processing still needs an Article 6 legal basis grounded in law and, where restrictions are imposed, compliance with the conditions of Article 23 and the Charter. AMs 1005 and 1011 appear instead to create a presumption that processing related to national security, military or defence tasks falls within Article 6(1)(e). Whatever their ultimate legal effect, this plainly does not simplify the GDPR. Because it inserts highly sensitive state-processing questions into a general simplification file and risks blurring the line between activities outside EU-law scope and public-authority processing that remains subject to EU data-protection guarantees.

Simplification that actually looks like simplification

AMs 349, 387, 1000, 1165, 1239, 1241–1242, 1342, 1347, 1593

Some amendments address compliance friction without weakening substantive rights. AM 1593 is the clearest example: it creates voluntary, standardised and machine-readable SME templates for information, documentation and notification duties and requires accessible guidance from supervisory authorities, while expressly preserving controllers' and processors' underlying responsibility. This is what simplification should look like: make compliance easier to understand and operationalise rather than exempting smaller actors from the law.

The same logic supports shared expertise, albeit the novelty should not be overstated given that Article 37(6) GDPR already allows a DPO to act under a service contract, and the same external DPO can serve several controllers. AM 349 and AMs 1239 and 1242 clarify or facilitate pooled arrangements more than they create a new simplification. AM 1241 adds a useful conflict-of-interest rule where the same DPO serves several controllers. That protection is sensible because the GDPR says little about conflicts between different client controllers, but technically it is also a new controller obligation rather than pure burden reduction. The better claim is that these amendments can make an existing compliance model clearer and safer, not that shared DPOs are currently impossible.

Other useful ideas improve transparency in complex data chains. AM 387, AM 1000 and AM 1165 would strengthen provenance duties for data obtained from brokers or other commercial intermediaries, while AM 1342 gives those duties meaningful enforcement consequences. AM 1347 would create a public data protection data space containing decisions, statistics and guidance. These measures reduce information asymmetry rather than rights.

Do not turn company size, non-profit status or 'low risk' into an off switch for rights

AMs 224, 229, 231, 347, 923–924, 926, 976, 981, 987, 1001, 1098, 1345, 1596, 1601

A broad amendment family tries to reorganise GDPR protection around categories of small, medium and large controllers. AMs 224, 229 and 231 provide the political framing; AMs 976, 981, 987 and 1001 create the size taxonomy; and AM 923 then uses it to exempt small controllers from duties including portability, record-keeping, DPIAs and governance requirements. AM 1098 adds a special proportionality clause across Chapter III rights, while AM 1345 caps fines for all infringements by small controllers at EUR 50,000.

The problem is not proportionality: the GDPR already uses risk, scale, context and resources throughout. The problem is replacing the risk of the processing with a proxy based on the organisation. A ten-person company can still process biometric data, monitor workers or make consequential decisions; a large organisation can carry out low-risk processing. Rights should follow what is done to people, not the headcount or turnover of the controller.

AM 924 and 926 need to be read together: AM 924 removes broad categories of processing from the GDPR, including low-risk processing and all processing by micro, small and medium-sized enterprises, and AM 926 then instructs Member States to ensure that processing excluded from the GDPR is covered by other bodies of law, including privacy, contract, tort, consumer, labour, unfair-competition and criminal law. The package therefore does not remove regulation but removes the harmonised GDPR framework and asks 27 national legal systems to reconstruct protection through different legal fields. That creates new legislative work, new conflict-of-law questions and fragmentation across the Union. AMs 1596 and 1601 pursue similar logic for voluntary and non-profit activity, and AM 347 proposes broad relief for civil society and volunteer organisations. Helping small or non-profit organisations comply is legitimate; declaring whole categories of processing outside the GDPR is not, and is likely to be contrary to Article 8 of the Charter of Fundamental Rights.

A rights-free zone for industrial data?

AMs 295, 1597

AM 295 creates a presumption that operational data from connected industrial equipment is lower-risk. AM 1597 then gives that idea legal teeth by disapplying Articles 15–22, 30 and 35 for a broad class of machine and industrial-IoT processing used for operation, maintenance, monitoring, improvement or security, subject to some safeguards and exclusions.

This is dangerous: **data generated by a machine can still be personal data.** For instance, factory telemetry can reveal which worker operated a machine, at what speed, with what errors and during which shift, or vehicle data can reveal a driver's movements and conduct. Pseudonymisation reduces risk but does not make those rights unnecessary or take the data outside the GDPR. **Industrial origin is not a reason to create a parallel, rights-light data-protection regime.**

The GDPR does not need 'privileged processing' or a catalogue of blessed legitimate interests

AMs 489, 1012, 1073, 1595

As mentioned earlier, the legitimate-interest test is deliberately contextual. AM 1595 would instead create a non-exhaustive annex of activities described as legitimate interests, including workplace monitoring and productivity, AI training, intra-group transfers (transfers or sharing of personal data between companies belonging to the same corporate group,), product improvement and marketing measurement.

AM 1012 takes the same direction by giving particular weight to anonymisation and intra-group transfers (the latter undermines the principle of purpose limitation), while AM 1073 creates an extensive new 'privileged processing' regime for intra-group administration, ordinary SME commercial processing and research or statistics: it actually requires entry in a register, approved codes or certification, creates presumptions across Articles 6, 9 and 46, and gives the Commission further delegated powers. If this is simplification, it comes with a registration form, the structure recalling the kind of processing-registration logic that the GDPR largely moved away from when it replaced Directive 95/46. AM 489 supplies the recital-level political framing. These approaches risk turning a contextual test into a list of politically pre-approved purposes. The fact that an activity can sometimes pursue a legitimate interest does not mean that it is necessary or that people's rights do not override it in a particular case.

PETs are safeguards, not permissions

+ AMs 1340

− AMs 1159, 1170, 1604

Another new amendment family treats privacy-enhancing technologies as a route to presumptive legality. AM 1159 would give the Commission a broad role in setting technical specifications for PETs across questions that include pseudonymisation, anonymisation and risk mitigation. AM 1170 would create a rebuttable presumption of compliance with data minimisation where certified PETs are used. AM 1604 would deem further processing carried out solely to anonymise data automatically compatible with the original purpose and lawful on the same legal basis.

As mentioned above, **PETs should be encouraged, but none of these technical measures answers the prior legal question.** Pseudonymisation does not create a lawful basis; encryption does not make an incompatible purpose compatible; and processing sensitive data in order to anonymise them still requires lawful processing before the anonymous output exists. AM 1340 points in the better institutional direction by keeping guidance on pseudonymisation, anonymisation and residual identification risk with the EDPB.

Put responsibility upstream when product design makes compliance impossible

+ AMs 1171, 1348, 1351, 1354

One of the more interesting new ideas is to recognise that controllers often depend on products and software designed by other actors. AM 1171 would require manufacturers to design products, services and applications so that controllers and processors can comply with the GDPR by default and obtain the information needed for their own obligations. If Parliament creates such direct manufacturer duties, remedies should follow them: AM 1348 extends judicial jurisdiction to manufacturers, AM 1354 adds manufacturer liability for damage caused by their acts or omissions, and AM 1351 allows a controller or processor that has compensated the person to seek contribution from a responsible manufacturer.

That is a potentially useful correction to current supply-chain asymmetries. It should not, however, become an excuse to remove the controller's own responsibility. AM 1175, should therefore receive a more balanced assessment. Its direct statutory processor duties can strengthen the position of controllers and reduce the need to reproduce every Article 28(3) obligation contractually. The concern is not that processor duties would automatically weaken controller duties, but its reach and allocation. Many processors, especially infrastructure providers outside the Union, may not be directly subject to every GDPR obligation on the same territorial basis as the controller. The current Article 28 contract can therefore transmit instructions and duties through the processing chain even where direct statutory reach is uncertain. AM 1175 also makes the detailed contract optional, creates rules on unfair processor terms and allows the Commission to specify further unfair terms. A sensible reform could place stronger direct duties on powerful processors while preserving a mandatory mechanism that binds non-EU and sub-processors and records the concrete instructions, purposes and allocation of responsibilities. Direct duties and a usable Article 28 agreement are complements, not substitutes.

Consent and data minimisation can be made easier for people too

AMs 1002, 1004, 1007, 1013, 1015, 1017, 1131, 1160, 1173

Several amendments use the Omnibus to simplify the user side of data protection rather than only the controller side. AM 1002 updates Article 7(2) so that consent requested through a digital interface must be clearly distinguishable for each purpose and from other matters. Concretely, a smart-TV setup, mobile-app sign-up flow or website should not be able to hide consent to advertising, profiling or AI training inside acceptance of general terms and conditions. AM 1004 states expressly that refusing consent must be as easy as giving it. AM 1007 requires neutral presentation of choices and targets dark patterns, while AM 1017 develops a more complete framework against manipulative consent interfaces. AM 1013 would require guest access where a permanent account is not strictly necessary, reducing the routine collection of identifiers and account histories merely to buy a product or use a service.

AM 1015 is also useful in making the legitimate-interest test more explicit: a real and precisely articulated interest, necessity including less intrusive alternatives, and an actual balancing against rights and expectations. These ideas clarify existing principles rather than inventing new permissions.

Child-specific amendments such as AMs 1131, 1160 and 1173 also contain useful safeguards, particularly where the trigger is a service likely to be accessed by children rather than an obligation to verify every user's age. AM 1131 nevertheless needs tighter drafting: by adding 'notably where the data subject is a child' to the requirement that an objection be based on grounds relating to the person's particular situation, it may imply that childhood itself supplies those grounds. That can strengthen children's ability to object, but Parliament should ensure it does not inadvertently narrow the grounds available to other data subjects or confuse the separate ex ante legitimate-interest balancing test, where the controller must already give particular weight to the fact that the person is a child. The objective is strong protection without creating an age-verification incentive or weakening other people's Article 21 rights.

Enforcement should be easier to use, not easier to avoid

+ AM 1341

− AMs 1311, 1312, 1316, 1320, 1352, 1357

Some amendments improve access to regulators, addressing one of the main insufficiencies of the data protection framework these years, that is, enforcement. AM 1341 would allow a complaint where unlawful processing is imminent or expected in the near future, rather than making people wait for deployment and harm. That is particularly valuable for large-scale or automated systems where the consequences may be difficult to reverse.

Others move the opposite way. AM 1352 makes a complaint inadmissible where the controller has a DPO unless the person first uses the internal channel and waits up to a month. AM 1312 expressly makes the extent of DPA investigation discretionary, while AM 1316 allows mandatory electronic complaint forms. Each shifts friction from the regulated actor to the person seeking a remedy. A DPO is an internal compliance function, not a mandatory first-instance tribunal, and digital-only complaint channels can exclude precisely the people who most need an accessible authority.

The institutional amendments are important to consider too. AM 1311 would prevent national DPAs from issuing guidance where the EDPB has already spoken, even where domestic law or sectoral context requires further explanation. AMs 1320 and 1357 would impose new procedural and policy requirements on the EDPB, including weighing innovation, competition, law enforcement and national security and operating a permanent stakeholder panel. Coordination is useful; importing economic and security objectives into an independent data-protection (a fundamental right) body's mandate would fundamentally alter its mission and scope.

Collective enforcement and compensation are not optional extras

+ AMs 1349, 1350, 1351, 1354

− AMs 1353, 1356, 1603

Data protection violations are often systemic by design in most of today's internet. Yet the harm experienced may be difficult to identify, prove or quantify, and the cost and complexity of bringing a case alone can easily exceed what any one person could realistically recover. This is exactly why **collective enforcement matters: it helps correct the enormous imbalance between organisations that control the data, systems and evidence, and the people affected by them.**

Article 80 GDPR allows qualified non-profit organisations to represent data subjects in complaints and judicial proceedings. AM 1603, which would delete Article 80 GDPR altogether, would therefore remove one of the Regulation's most important mechanisms for turning rights on paper into rights that can actually be enforced. AM 1353 would narrow that model by preventing representative bodies from pursuing compensation claims under Article 82. Both moves would make enforcement more individualised precisely where the underlying violations are often collective. The compensation debate under Article 82 raises the same concern. AM 1356 would introduce a 'significant impairment' threshold for non-material damage. That risks excluding precisely the kinds of cumulative or intangible harms that are common in data protection: loss of control over personal data, unlawful disclosure, persistent tracking, exclusion, profiling or the chilling effects of surveillance.

Other amendments strengthen the sanctions that can be imposed on an infringing controller by not setting sanctions lower that the profits derived from the infringement (AM 1349), adding criminal sanctions where appropriate (AM 1350), and allowing a controller to seek compensation from other controllers, processors and manufacturers corresponding to their part of responsibility for damages the controller has paid to a data subject (AM 1351 and AM 1354).

Do not lower the international-transfer standard through a 'simplification' file (or at all)

AMs 1307–1309

AMs 1307 and 1308 are more problematic than a generic reference to a 'risk-based' transfer framework suggests. AM 1307 rewrites Article 44 by replacing the current command that the level of protection guaranteed by the GDPR must not be undermined with a new standard that protection in the third country must be 'not materially lower.' It then creates an internal contradiction: new paragraph 1a says data subjects must still receive protection 'essentially equivalent' to that guaranteed in the Union, which is the CJEU standard the first paragraph has just weakened, and refers to technical and organisational measures as part of the assessment. Technical safeguards can reduce some transfer risks, but they cannot by themselves cure third-country laws that compel access to data in ways incompatible with EU fundamental rights. New paragraph 1b adds a rebuttable presumption that common internal standards or binding rules within multinational groups satisfy Article 46. That can particularly benefit large multinational groups, while the central problem remains external law: a company's internal rule cannot bind a third-country intelligence or law-enforcement authority. AM 1308 then imports the 'not materially lower' formula into adequacy decisions

and removes parts of the current urgent suspension machinery. AM 1309 is a consequential part of that package. This is not administrative simplification in the least but a substantive change to the threshold governing when personal data can leave the EU. What is more, **the existing adequacy standard is anchored in the Charter and CJEU case law, hand in hand with international commitments. Technical or organisational safeguards could reduce some risks in a transfer, but they cannot make incompatible foreign surveillance law disappear.**

Data brokers: prove where the data came from

AMs 387, 1000, 1165 and 1342

AMs 387, 1000, 1165 and 1342 address a real accountability gap in data-broker chains. AM 387 states the underlying principle clearly: when a controller buys, aggregates, enriches, sells or otherwise obtains personal data through third parties, accountability requires it to verify and document the lawful origin and legal basis of the data rather than accepting a generic supplier assurance. AM 1000 makes that duty operative and says a general compliance declaration or standard contractual term from the provider cannot be enough. AM 1165 adds provenance information to records of processing, and AM 1342 makes clear that failures in this area fall within the serious-infringement fine tier. These amendments largely clarify what Articles 5(1)(a), 5(2) and 24 should already mean in an opaque broker chain: unlawfully collected personal data cannot be laundered into legality simply by passing through successive intermediaries.

That clarification could **materially improve much needed enforcement against data brokers,** including chains involving providers established outside the EU, because the EU controller that buys or onward-processes the data would have an express verification duty and could not hide behind contractual assurances from an upstream broker. The drafting still needs coordination with Articles 13, 14, 24 and 30, and enforcement against actors with no meaningful EU presence remains difficult. Those implementation questions do not undermine the core idea: requiring the party that wants to profit from third-party data to prove where the data came from is a direct way to place the evidential burden on the actor with access to the commercial chain rather than on the person whose data were traded.

11. Acronyms

AI	Artificial intelligence
AM	Amendment
CJEU	Court of Justice of the European Union
DPA	Data protection authority
DPIA	Data protection impact assessment
DPO	Data protection officer
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EP	European Parliament
EPD	ePrivacy Directive
EUDPR	EU institutions' data-protection regulation
GDPR	General Data Protection Regulation
GPAI	General-purpose AI
ITRE	EP Committee on Industry, Research and Energy
LED	Law Enforcement Directive
LIBE	EP Committee on Civil Liberties, Justice and Home Affairs
MEP	Member of the European Parliament
PET	Privacy-enhancing technology
SME	Small and medium-sized enterprise
SMC	Small mid-cap company

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram



EDRi
European Digital Rights