CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Bonn, Bucharest, Dublin, Lisbon, Luxembourg, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

Omnibus Survey Report
Analysis of the CEDPO Questionnaire on Omnibus IV and VII

March 2026

Contact information:
https://cedpo.eu
info@cedpo.eu

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Contents

Introduction

This report analyses the results of a survey conducted by the Confederation of European Data Protection Organisations (CEDPO) in response to the European Commission's "Omnibus IV and VII" proposals affecting data protection and digital regulatory frameworks.

The survey gathered feedback from data protection professionals and stakeholders on 29 proposed legislative and regulatory adjustments, focusing primarily on implications for the interpretation and application of EU data protection law. Overall, the results reveal a cautious and often critical response from practitioners, particularly when proposals risk weakening legal certainty or reducing protections for data subjects, while more operational or harmonization-oriented measures receive comparatively stronger support.

Methodology and Respondent Profile

The questionnaire collected responses from 672 participants. Respondents consisted mainly of privacy professionals, data protection officers (DPOs), compliance experts, and legal practitioners working in organizations subject to EU digital regulation across the EU27. In addition to quantitative responses (agreement levels), qualitative comments were analysed to capture deeper professional concerns, reflections, and operational perspectives. Across questions, qualitative feedback often expressed stronger positions than the numerical results, with a high proportion of critical commentary even where agreement levels appeared moderate. We have included a selection of positive as well as negative comments per question to highlight and demonstrate the spectrum of feedback and reflection received.

The questionnaire was carried out in several EU languages, namely English, French, German, Italian, Spanish and Romanian.

Some Key Findings

1. Strong Concerns Regarding Changes to the Definition of Personal Data

The proposal to clarify the definition of personal data by incorporating elements derived from case law received the most negative feedback. While around 28% of respondents expressed agreement with the proposal, a majority disagreed or strongly disagreed. Approximately 88% of the comments analysed were negative.

Respondents acknowledged the intention to introduce a more pragmatic "in concreto" approach based on whether a specific actor can reasonably identify a person. However, several major concerns emerged:

- **Legal uncertainty:** The proposed wording was considered ambiguous and overly dependent on subjective assessments (e.g., "reasonably likely"), potentially leading to inconsistent interpretations across organizations and regulators.
- **Risk of misuse:** Respondents feared that the flexibility could enable organizations to classify identifiable data as non-personal depending on the recipient's capabilities, thereby weakening compliance obligations.
- **Operational complexity:** Contrary to the objective of simplification, many practitioners predicted additional workload for DPOs who would need to assess identification risks case-by-case.
- **Impact on data subject rights:** Respondents highlighted that the proposal might reduce individuals' control over their personal data and weaken accountability mechanisms within processing chains.

Overall, stakeholders strongly emphasized that the current definition of personal data is widely understood and legally stable, and that modifying it could introduce unnecessary complexity.

2. Mixed but Cautiously Positive Reception for Clarification on Pseudonymised Data

The proposal granting the European Commission authority to adopt implementing acts defining criteria under which pseudonymised data may no longer be considered personal data received a more balanced response. Approximately 47% of respondents agreed or strongly agreed with the proposal, while roughly 28% disagreed.

Supporters emphasized several benefits:

- **Operational clarity:** Clear criteria for assessing re-identification risk could help organisations determine when pseudonymised data may be used more flexibly.
- **Harmonisation:** Common EU-wide standards could reduce fragmentation in regulatory interpretation across member states.
- **Facilitation of data use:** Greater clarity may enable safer and more efficient data sharing in research and innovation contexts.

However, many respondents remained cautious. Nearly 80% of the written comments expressed concerns, including:

- potential over-simplification of complex technical issues related to re-identification,
- the need for robust safeguards against future identification,
- uncertainty about how implementing acts would interact with existing guidance.

Overall, while stakeholders recognize the need for clearer rules, they stress that any framework must remain technically robust and aligned with evolving technological risks.

3. Broad Support for Regulatory Harmonisation and Administrative Simplification

Several proposals aimed at harmonizing definitions across EU digital legislation or simplifying administrative processes received relatively positive feedback.

In particular, respondents showed interest in:

- **Uniform definitions across EU digital laws** (e.g., terms related to electronic communications, online interfaces, and media services), which could reduce interpretive discrepancies across overlapping regulatory frameworks.
- **A single reporting entry point and standardised templates** for compliance reporting under multiple regulatory regimes (including cybersecurity and digital resilience frameworks).

Professionals consistently highlighted the growing regulatory complexity organizations face due to overlapping EU instruments. Harmonization initiatives were therefore viewed as potentially valuable for improving legal clarity and reducing administrative burdens.

Nevertheless, respondents stressed that simplification should not compromise substantive data protection requirements. Clear governance mechanisms and coordinated implementation across authorities would be necessary to ensure consistency.

4. Divergent Views on Data Breach Notification Reforms

Proposals concerning data breach notification obligations generated mixed responses. Suggestions such as extending the breach notification deadline from 72 to 96 hours or limiting reporting obligations to cases involving high risks to data subjects were seen by some as practical improvements that could reduce unnecessary reporting pressure.

However, others warned that loosening reporting requirements might weaken transparency and oversight. Several respondents argued that supervisory authorities should retain strong visibility into security incidents, even when the risks to individuals are not immediately clear.

Similarly, proposals to create common templates and harmonized EU-wide criteria for breach notifications were generally welcomed as a way to improve procedural consistency across member states.

5. Recurring Cross-Cutting Themes

Across the survey, several recurring themes emerged:

- **Demand for legal certainty:** Practitioners consistently prioritized clear, stable definitions and predictable compliance obligations.
- **Concern about weakening protections:** Many respondents expressed strong opposition to reforms perceived as potentially reducing safeguards for individuals.
- **Support for practical harmonization:** Measures aimed at simplifying administrative processes, aligning terminology across EU laws, or improving procedural consistency were generally welcomed.
- **Recognition of technological complexity:** Respondents emphasized that regulatory reforms must account for evolving risks related to artificial intelligence, cybersecurity, and large-scale data analytics.

6. Cumulative deregulatory effect

Respondents consistently warned that even individually acceptable proposals may, taken together, produce a cumulative weakening of the GDPR framework. This systemic concern — expressed across questions on personal data definition, special categories, automated decision-making, ROPA and breach notification — should be read as a structural signal, not merely a sum of isolated objections.

Overall Assessment and Conclusion

The survey results indicate that EU data protection professionals are open to reforms that enhance clarity, harmonization, and operational efficiency. However, they remain highly cautious toward proposals that modify core legal concepts or introduce interpretive ambiguity.

In particular, the proposed reformulation of the definition of personal data is widely viewed as problematic and potentially destabilizing for the current legal framework. By contrast, targeted technical guidance—such as standardized procedures, harmonized reporting mechanisms, and clearer criteria for pseudonymisation—has stronger potential to improve compliance practices without undermining fundamental protections.

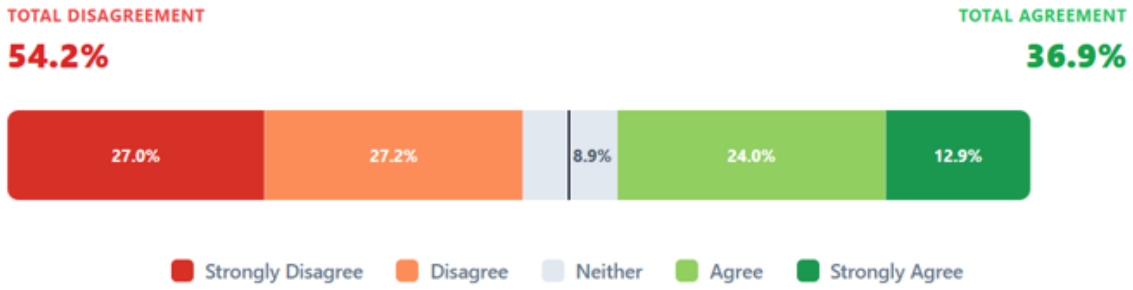
The feedback gathered through the CEDPO questionnaire highlights the importance of balancing regulatory modernization with legal stability. While stakeholders recognize the need to adapt the data protection framework to technological and regulatory developments, they emphasise that reforms should reinforce clarity and accountability rather than introduce new uncertainty.

Future legislative initiatives should therefore prioritise operational harmonization and technical guidance while preserving the foundational principles of the EU data protection regime.

Results Analysis

Question 1: Proposal to clarify the definition of personal data based on the definition presented in the CJEU ruling (C-413/23 P EDPS v SRB).

Quantitative results:



Positive comments:

- **A not entirely favourable reception**: the reception of this amendment is generally favourable in substance, as it simplifies operations, particularly regarding the management of internal identifiers and the fluidity of data exchanges. While the logic of the *in concreto* approach (linked to the actual ability of the data controller to identify a person) is welcomed, the current wording is considered too cumbersome and the last sentence of the text is strongly contested, as it could allow sensitive data to circulate without legal supervision when a subsequent recipient is involved.

Negative comments:

On formulation: A lack of intelligibility

- **Lack of clarity:** The current wording raises issues of overall comprehensibility and legal predictability. The use of terms such as "reasonably likely," "not necessarily", "mere fact" or "merely because" is strongly criticized because it leaves too much room for subjective interpretation.
- **Negative approach:** The very structure of the definition (defined by what it is not) hinders its readability.

Fundamental issue: Legal and operational uncertainty

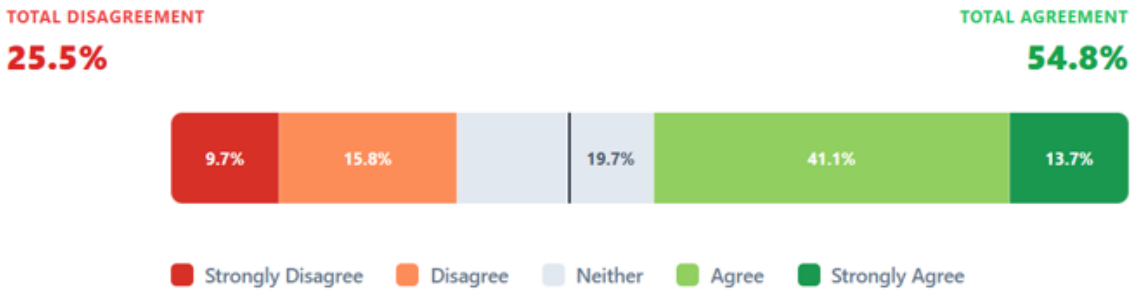
- **Increased subjectivity:** The shift from an objective definition to one based on the recipient's capabilities makes data classification uncertain ("variable geometry" definition). There is a risk of interpretative fragmentation by introducing an assessment that depends on each entity, which can lead to divergent interpretations between controllers and supervisory authorities, especially in shared data ecosystems.
- **Risk of misuse:** Contributors fear that this flexibility could be exploited to bypass GDPR requirements and weaken personal data protection.
- **Misunderstanding of technical issues:** The text ignores the reality of data cross-referencing and the new risks associated with artificial intelligence and cybersecurity.
- **Enhanced complexity for the profession:** Far from simplifying processes, this change increases the workload of DPOs. In fact, comments highlight that although the definition may be more in line with reality, it requires an analysis that is difficult to carry out in practice, which will probably result in less data protection, as data will be considered non-personal by default. For SMEs, it would be desirable to incorporate objective criteria that reduce the interpretative burden.

On the enforcement of rights: A major setback

- **Reduction of personal data protection:** Several comments express concern over the erosion of the right to data protection and the loss of protection and transparency, rendering fundamental principles such as proactive responsibility, loyalty and transparency meaningless. It is considered that the reference to means "that may reasonably" be used renders the definition of personal data meaningless. The amendment results in a loss of control for the data subject and weakens the chain of responsibility among stakeholders.
- **Challenging the acquis:** The current definition is considered clear and widely accepted; changing it would create uncertainty where none existed before.
- **Uncertain anonymization:** The text does not guarantee against subsequent identification; contributors argue that data should be considered personal whenever identification is possible, regardless of who processes it. The proposal is also criticised for not containing any specific exceptions or safeguards.

Question 2: Proposal to empower the Commission with the authority to adopt implementing acts to specify means and criteria to determine whether data resulting from pseudonymisation no longer constitutes personal data for certain entities.

Quantitative results:



Positive comments:

A favourable reception in terms of principle and usefulness

- **Operational relevance:** The measure is considered relevant by professionals. The objective of clarification and harmonization is welcomed as a way to reduce the current uncertainty surrounding the risks of re-identification and reducing the risk of excessive compliance due to defensive prudence.
- **Progress compared to the existing situation:** The introduction of new standards and criteria is seen as a net gain for better practice, enabling a shift from an obligation of means to greater visibility on the expected results.
- **Recognition of the dynamic nature of risk:** The proposal recognises that pseudonymisation is not binary in nature but rather depends on the context, the actor and the technological environment, through explicit reference to the state of the art and risk assessment according to typical recipients.
- **Simplification of exchanges:** Respondents emphasize that these measures could facilitate data exchanges and the use of pseudonymized data when re-identification is deemed impossible for the recipient.

Negative comments:

Legal and operational uncertainty

- **Source of complexity**: Far from simplifying the task, the addition of new texts is perceived as a threat to the readability of the law.

- **Inadequacy to technical developments:** Technology, particularly AI, is evolving faster than the legislative process. Setting fixed criteria in implementing acts is considered risky; many opinions prefer to leave it up to data controllers to adapt to the state of the art.
- **Time-consuming case-by-case approach:** An approach based on examining specific situations is considered too cumbersome and ineffective in practice.

Doubts about legitimacy and governance

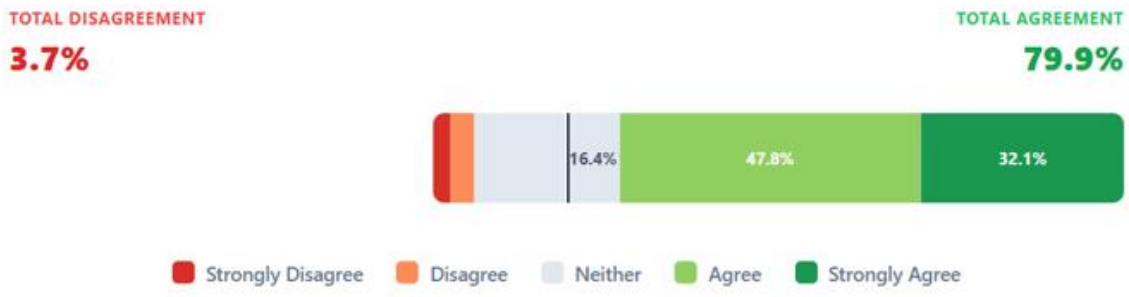
- **Risk of lobbying:** The authority entrusted to the European Commission raises concerns about the influence of lobbying groups at the expense of data protection.
- **Weakening of supervisory authorities:** Contributors are concerned about the loss of influence of supervisory authorities and are calling, at the very least, for the opinion of the EDPS to be binding and for a double control system to be introduced.
- **Lack of transparency:** The procedures for referring cases to the Commission and establishing decision-making criteria remain too vague, creating a lack of transparency in the process. A recurring structural concern is that the proposal assigns implementing powers to the Commission without making the EDPB's opinions binding. Respondents broadly agree that the EDPB should have sort of formal veto or co-decision role, rather than merely advisory standing, to preserve supervisory independence.

A challenge to the very principle

- **Nature of the data:** One particular argument is consistently recurrent: Pseudonymization is, by its very nature, reversible. As long as re-identification is possible, the information remains personal data and should not be subject to exemptions**.**
- **Text ambiguity:** The current wording is considered too vague to offer robust and effective guarantees. Without strict safeguards, the measure is seen as opening the door to the misuse of GDPR principles.
- **Risk of equating with anonymisation:** There is a concern about whether pseudonymisation would now be equivalent to anonymisation, when that distinction is made in the current regulations for a reason.

Question 3: Proposal to use uniform definitions in different EU digital laws for 'terminal equipment', 'electronic communications networks', 'web browser', 'media service', 'media service provider', 'online interface'.

Quantitative results:



Positive comments:

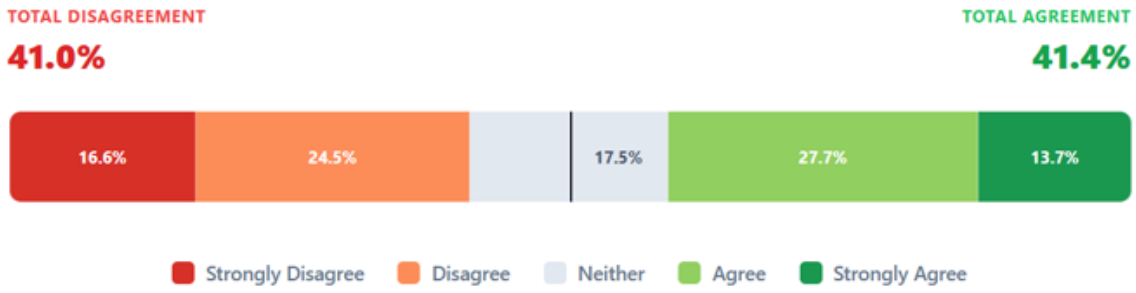
- **Inter-textual consistency:** The urgent need is to ensure that the concept of personal data remains the same, regardless of the applicable rule: This approach helps to stabilise the overall legal framework.
- **Security and clarity:** Harmonization is seen as the "minimum requirement" for dispelling current legal uncertainty and providing greater visibility for stakeholders. Aligning concepts provides immediate clarity, making compliance easier for data controllers.
- **Sectoral regulatory specialisation : R**eference to definitions contained in specific sectoral regulations is legally correct and prevents the GDPR from becoming an autarkic or siloed text disconnected from the rest of the digital acquis.
- **Real simplification:** This approach fulfils the objective of simplification by avoiding divergent interpretations across sectors or regulations. Maintaining divergent definitions for identical technical concepts creates unnecessary interpretative difficulties.
- **Consistent application:** A single definition allows for more consistent application of obligations across different data processing operations.
- **Cost reduction for SMEs :** Digital SMEs would benefit from operating in several simultaneous regulatory frameworks with uniform definitions, significantly reducing the burden of duplicate legal analysis, the risk of unintentional non-compliance and reliance on ad hoc interpretations.

Negative comments:

- **Complexity of cross-references:** The decision to use cross-references rather than repeating terms has been heavily criticized. This method is considered time-consuming and detracts from the immediate readability of the text for practitioners. The proliferation of cross-references risks making the whole text incoherent and difficult to understand for non-experts.
- **Doubts about usefulness and consistency:** Vigilance is required to ensure that these definitions do not conflict with the general framework of the GDPR and respect its protective context. Some respondents believe that this amendment is unnecessary, considering it a minor detail with no real or beneficial impact on daily practice.

Question 4: Proposal for a definition of "scientific research" specifying that "research may also aim to further a commercial interest".

Quantitative results :



Positive comments:

- **Promoting progress:** This measure is considered necessary to encourage innovation. Stricter regulation of the concept would provide a secure framework for research projects.
- **Reality of R&D&I:** Recognition that applied research operates at the intersection between the general interest and commercial interests. This is considered to be stating the obvious, as research is never altruistic, especially when there is investment behind it. Commercial interests are often necessary in order to continue research activities.
- **Regulatory continuity:** Some contributors see this provision as equivalent to Recital 159 of the GDPR, thus ensuring consistency with the principles already established for scientific research.

- **Primacy of the public interest:** Approval is conditional on public interest remaining superior over private interests. The level of transparency towards citizens must be maintained or even strengthened.
- **Terminological adjustments:** Some proposals suggest a change in terminology to better reflect these issues and avoid confusion.
- **Priority for anonymization:** Several opinions specify that this broadening of scope should only be possible in the presence of truly anonymized data, in order to guarantee maximum security for the individuals concerned.

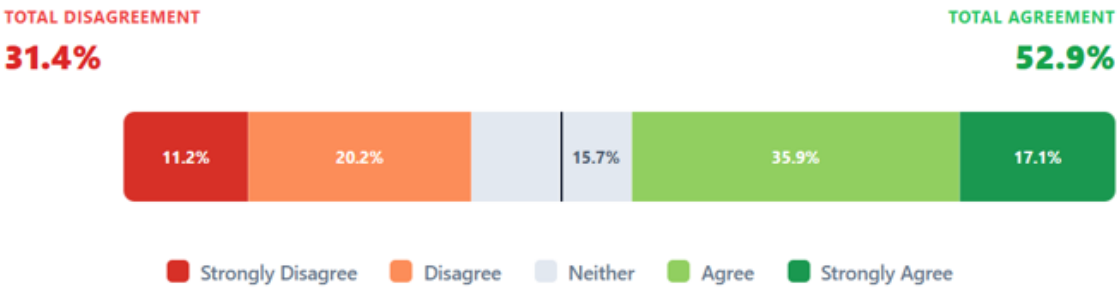
Negative comments:

- **Circumvention of the GDPR**: Many respondents fear that this definition could serve as a "pretext" for certain entities to benefit from exemptions from the GDPR and process data outside of any protective framework.
- **Uncertainty regarding commercial interest:** A major concern is the confusion between fundamental research and profit-driven research. There are calls to strictly separate these two scenarios, with much stronger security measures and consent requirements for commercial purposes.
- **Lack of clarity and need for improvement:** The concept of commercial interest in this definition is unclear. It is considered that the definition could be significantly improved. Scientific research is one thing, but the use of the results of such research for commercial interests is another.
- **Lobbying pressure:** Some opinions denounce a "mercantile" definition influenced by lobbyists, which would stray from a necessary scientific neutrality.
- **Uselessness and imprecision:** Some consider this addition unnecessary, as research is already defined by its methods (knowledge production) and not by its ultimate objectives.
- **The "common good" under threat:** Respondents point out that science is for the common good, which is considered incompatible with a purely commercial or proprietary view of data. Several comments express that it (the common good) loses its intended purpose and that commercial interests clash with fundamental rights.
- **Lack of safeguards**: The current definition is considered too broad and lacking sufficient safeguards to protect those concerned.
- **Peer review:** To avoid abuses, it is suggested that the "scientific" nature of a treatment must be confirmed by trusted third parties: scientific integrity experts, ethics committees, or peer review.

- **Need for ethical standards:** Importance of maintaining the requirement is noted to contribute to general knowledge or social welfare and explicit reference to ethical standards in the relevant field of research as material conditions; not merely declarative ones.

Question 5: Proposal to facilitate the possibility to reuse personal data for archiving, scientific or historical research or statistical purposes by considering It automatically compatible with the initial purposes, and without it having to pass the compatibility test of article 6(4) GDPR.

Quantitative results:



Positive comments:

- **Archiving and Statistics:** These purposes are considered consistent and low risk. Archiving in the public interest is seen as an administrative necessity, while statistics are secured by the principle of aggregation and statistical confidentiality.
- **Scientific research:** This is the main point of concern. Unlike the other two, this purpose is seen as "dangerous" because it complicates the exercise of individuals' rights. It can only be accepted on condition that the "scientific" nature of the research is rigorously documented with the DPO.
- **Maintaining compliance obligations:** Simplification must not in any way exempt stakeholders from accurately documenting their purposes.
- **Neutrality for DPOs:** Some believe that these measures will not have a negative impact on the DPO profession, provided that the documentation framework remains strict and clear.

Negative comments:

- **Opposition to private/commercial interests:** Contributors are categorical: if these provisions apply to commercial purposes, they must be rejected. The public interest must take precedence over private interests.
- **Risk of misuse:** The text is perceived as "very dangerous" for scientific research, as it could be used as a pretext for companies to bypass consent and individual rights.
- **Rejection of automaticity:** The idea of "automatic" compatibility of purposes is strongly criticized. Respondents fear the loss of a major safeguard in the GDPR, leading to a lack of predictability for citizens regarding the future use of their data. There is a risk that further processing materially deviates from the reasonable expectations of the data subject.
- **Maintaining the compatibility test:** The majority calls for the maintenance of a strict compatibility test and a case-by-case analysis, rather than a general presumption that would weaken individuals' rights. Removing this assessment weakens the principle of purpose limitation, one of the pillars of the GDPR.
- **Uselessness of the text:** Some consider the article useless, pointing out that respect for privacy and the obligation to document processing must apply regardless of the ultimate purpose.
- **Requirement for fairness:** Regardless of the nature of the organization (public or private), full compliance with the GDPR must remain the absolute standard for ensuring data protection.
- **Impact on vulnerable groups and sensitive data:** In contexts such as health, biometric data, neurodata or social data, reuse without a specific compatibility assessment can lead to high risks of stigmatisation, profiling or sensitive inferences, even for supposedly scientific purposes.
- **Destruction of fundamental principles:** There is concern that the proposal will completely destroy the principles of limitation, in addition to the data subject losing all control over the processing of such data. The principle of storage limitation will disappear. The proposal will render the principles of minimisation and purpose limitation ineffective.
- **A more balanced alternative:** A more GDPR-compliant approach would be to presume compatibility (rather than automatically imposing it), maintain a simplified compatibility test, or establish clear and harmonised criteria for its application in research, without completely removing it.

Question 6: Proposal to have a single-entry point and a common template for all incident reporting, not just under the GDPR but also for DORA, NIS2, eIDAS, CER.

Quantitative results :

Positive comments:

- **Harmonization and one-stop shop:** This proposal is widely acclaimed as a major time-saving measure. The implementation of a harmonized notification model via a one-stop shop is seen as a guarantee of efficiency for organizations. Indeed, a single point of entry allows for a holistic view of the incident, better coordination between competent authorities, and faster responses that are proportionate to the actual risk, benefiting both stakeholders and affected organisations.
- **Simplification and consistency:** Organisations, particularly SMEs, face fragmented reporting obligations with different deadlines, formats, and authorities. The project is considered consistent and significantly easier to implement. It helps to avoid data entry errors and significantly improves the operational management of incidents, and facilitate compliance in high-pressure operational situations
- **Extension of the deadline to 96 hours:** The change to a 96-hour deadline has been very well received. It is considered to be more in line with the reality of technical investigations, enabling more complete and accurate notifications to be sent to the authorities.
- **Cyber convergence:** The idea of creating "bridges" between different cyber regulations (such as NIS 2 and the GDPR) is welcomed.
- **Necessary uniformity:** However, this approval is conditional on strict and identical application in all Member States to ensure genuine equal treatment.

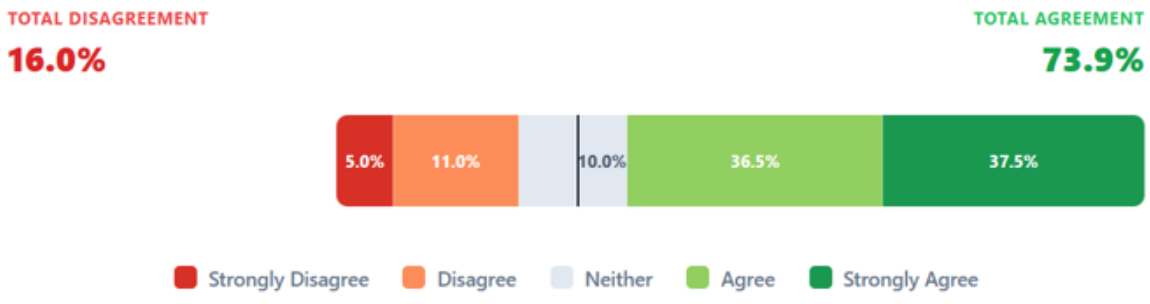
Negative comments:

- **Need for accessibility and clarity:** The functioning of the single entry point should be described in greater details and, if this is done, it should be made accessible and clear to those who are not familiar with DORA or NIS2.

- **Risk of confusion of competences:** A major concern has emerged regarding the one-stop shop: some fear that one authority may favor the application of one regulation over another (conflict of objectives between European texts).
- **Maintaining "data" jurisdiction:** Respondents strongly argue that the responsible data protection authority must remain the sole authority with jurisdiction to handle personal data breaches, to avoid any dilution of responsibilities.
- **Unclear boundaries:** The lack of clarity regarding the exact role of each actor involved raises fears that implementation will be much more complex than theory would suggest.
- **Concerns about delays and knowledge:** There is concern that a single point of entry could lead to delays in communications and that the new interlocutor may not have full knowledge of all the regulatory frameworks applicable to incidents. It is necessary to promote communication as soon as possible, even in cases of suspicion, rather than adhering to a maximum deadline.
- **Marginalization of the DPO:** Concerns have been raised about a loss of influence, oversight, or a reduction in the role of the DPO in this new notification system.
- **Side effects:** One participant is concerned about unforeseen consequences ("side effects") that could weaken the overall management of security incidents.
- **Contested deadline:** Despite the positive opinion of some, the new deadline is not unanimously accepted and remains contested by some respondents, who see it as a potential obstacle to the responsiveness required in a crisis.

Question 7: Proposal to increase the notification period for data breaches to 96 hours (instead of 72 hours).

Quantitative results :



Positive comments:

- **Pragmatic approach:** A realistic choice that prioritizes on-the-ground effectiveness.
- **Increased responsiveness:** Allows you to focus first on resolving the incident before dealing with administrative tasks.
- **Data quality:** Ensures richer, more detailed notifications thanks to hindsight.
- **Adequacy to operational reality:** In practice, many incidents require identification of the actual scope, preliminary forensic analysis, and risk assessment for stakeholders. An additional 24-hour margin allows for more complete and useful notifications, avoiding premature or inaccurate communications that generate subsequent burdens. The 72-hour deadline is not realistic based on experience with numerous clients. Management takes more than 72 hours.
- **Consistency with regulatory frameworks:** The extension to 96 hours is consistent with the logic of temporal harmonisation underlying the new digital resilience frameworks (NIS2, DORA). This facilitates the coordinated management of incidents in organisations subject to multiple regulatory regimes.
- **Maintenance of the principle of diligence:** It is positive that the obligation to notify without undue delay is retained, which prevents the new deadline from being interpreted as an automatic waiting period. The maximum deadline does not replace the duty to act immediately.

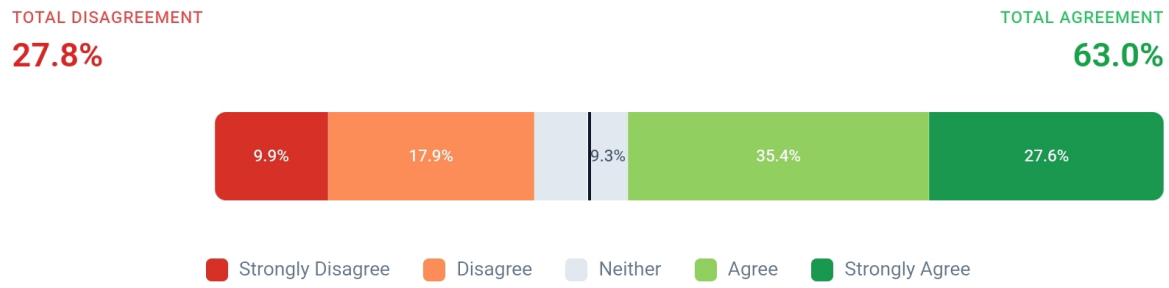
Negative comments:

- **Maintaining the 72-hour deadline**: Desire to keep the standard deadline, as it is always possible to complete an initial notification later.
- **Lack of justification:** Lack of arguments for extending the deadline and need to clarify whether the count includes weekends.
- **Risk of minimizing violations:** Danger of underestimating the significance of the data breach.
- **Impact on users:** A longer deadline is detrimental to those affected and would exacerbate the potential for harmful consequences.
- **Concern for high-risk situations:** In incidents with an immediate and significant impact on the rights of data subjects, speed remains essential. The increase in the deadline should not delay containment measures or postpone communication when the risk is already evident. In order to take action to minimise risks, it is necessary to report the incident as soon as possible. If urgent measures need to be taken, up to 96 hours is excessive.
- **Specific needs of SMEs:** Request to extend the deadline, particularly for small organizations with fewer resources.

- **Technical and terminological issues:** The problem is not whether it is 72 or 96 hours, but rather the use of the term "knowledge" versus "evidence," which adds a degree of certainty about the existence of the breach that is more reasonable.

Question 8: Proposal to limit the necessity to report personal data breach to DPAs to cases where it can result in a high risk to data subjects.

Quantitative results:



Positive comments:

- **Reduction in volume:** Avoids multiplying unnecessary alerts for minor violations with no real impact.
- **Risk targeting:** Refocuses the obligation solely on violations that pose a high risk to rights and freedoms.
- **End of "defensive" notifications:** Limits systematic reporting made simply out of fear of punishment.

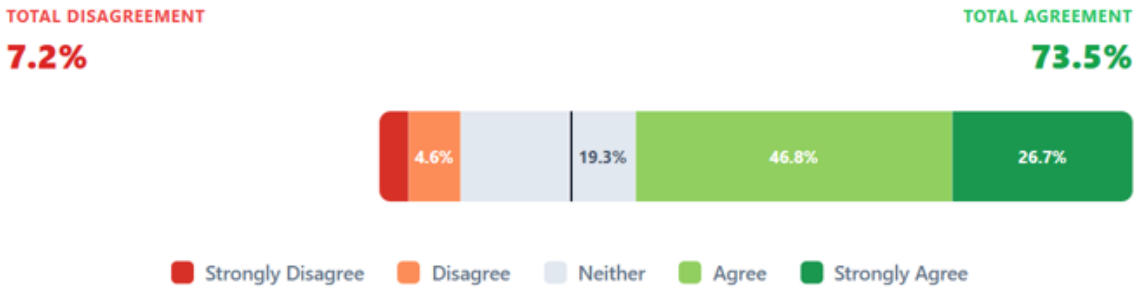
Negative comments:

- **Risk of underreporting:** Concerns about a lack of transparency and the need for more comprehensive legislation to prevent omissions.
- **Subjectivity of "high risk":** Too much discretion, making assessment of severity difficult and arbitrary. The importance of the DPO's prior assessment to determine whether or not there are risks remains critical.
- **Decreased accountability of stakeholders:** Risk of companies becoming less accountable and increased complexity for the work of the DPO.
- **Decreased vigilance:** Fear of a loss of overall security and less effective management of incidents without immediate implications.
- **Denaturalisation of the double threshold system:** The current regime is considered sufficient; moving to "high risk" is perceived as a step backward in terms of protection. Indeed, unifying both thresholds reduces the authorities' capacity for early supervision.

- **Relevance of 'non-high' risk from a systemic perspective:** Many breaches that individually do not reach the "high risk" threshold reveal structural weaknesses, allow patterns of non-compliance to be identified, or have cumulative effects. Excluding them from notification limits the preventive and guiding role of supervisory authorities. It will limit knowledge of incidents and make it quasi impossible to determine the trend of breaches, controls, and countermeasures.
- **Increased discretion and legal uncertainty:** transferring the sole decision on whether an incident is "high risk" to the controller increases decision-making pressure at critical moments, raises the risk of misclassification, and may lead to ex post penalties for under-reporting. Paradoxically, this does not reduce the burden, but rather shifts it and makes it more uncertain.
- **A more balanced alternative:** To alleviate the administrative burden without weakening the system, simplified forms for low-risk incidents, clear guidance from the EDPB on risk assessment, or staggered reporting thresholds, but not eliminated thresholds, would be preferable.

Question 9: Establish a transitional regime for security breach notifications, maintaining direct reporting to supervisory authorities until the NIS2 Directive's single point of entry is operational, thereby ensuring continuous reporting.

Quantitative results:



Positive comments:

- **Transitional relevance:** Ensures continuity of notifications and avoids legal uncertainty before the complete switchover.
- **Legal certainty:** Guarantees a single, fully functional NIS2 entry point before removing the old channels.
- **Pragmatic nature:** Measure deemed logical and essential for the smooth running of the process.

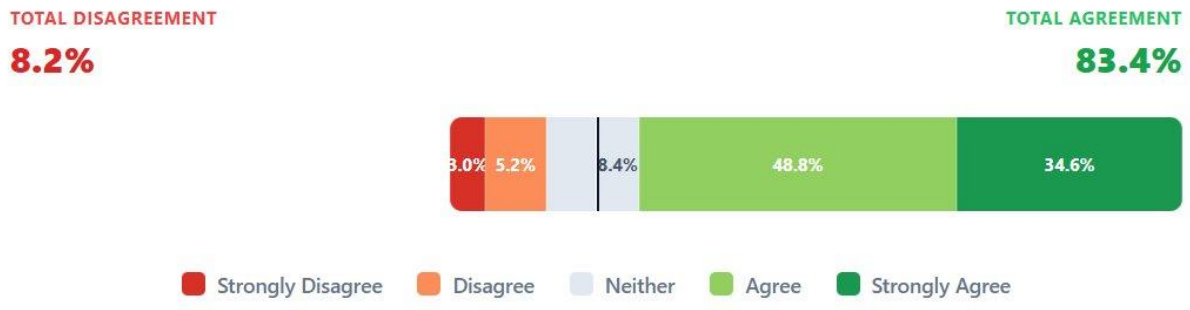
- **Special protection for SMEs:** SMEs cannot cope with periods of regulatory ambiguity or invest in provisional systems, this solution offers a clear, simple and proportionate framework.

Negative comments:

- **Risk of increased complexity:** The accumulation of standard-based provisions creates an overly complicated system; the current regime is sufficient until NIS2 comes into force.
- **Lack of clarity:** Need to clarify the role of the authorities and harmonize referral procedures to avoid confusion.
- **Concerns about effective implementation:** There is concern about the need to establish specific deadlines, as the experience in several Member State suggests that, without established deadlines, administrations do not effectively implement the systems.

Question 10: Proposal to mandate the EDPB to develop a common breach notification template and a single list of high-risk circumstances, to be adopted by the Commission via implementing acts, to harmonize EU-wide criteria and procedures.

Quantitative results:



Positive comments:

- **European harmonization:** A useful lever for improving consistency between countries and reducing administrative burdens.

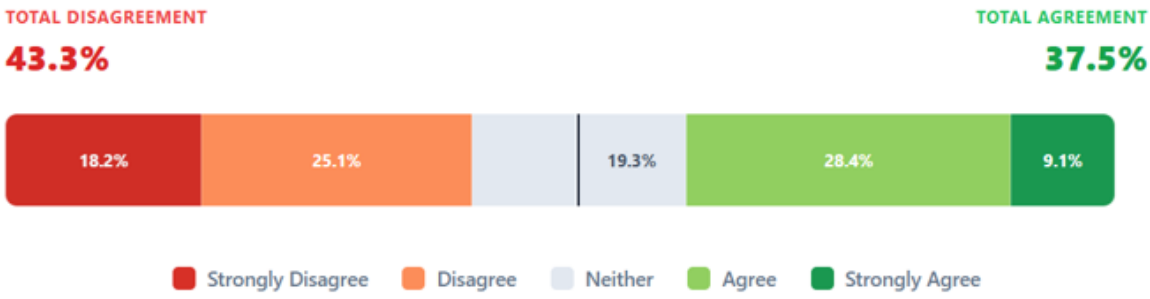
- **Improving the quality of notifications:** A common template facilitates more complete and comparable notifications, more efficient analysis by the authorities, and a faster and more proportionate supervisory response.
- **Relevance of review:** The principle of regularly reevaluating measures is considered a good initiative. It prevents the template and criteria from becoming obsolete in an environment of changing cyber threats and new processing models, although some comments consider the review period to be too long, especially for the list.
- **Qualification assistance:** Valuable support for better defining and classifying the nature of data breaches.
- **Appropriate institutional balance:** The EDPB's contribution of technical, practical and supervisory expertise is viewed positively, while the Commission ensures formal adoption and consistency with the EU regulatory acquis.
- **Clarity in high-risk assessment:** A single list of high-risk circumstances reduces excessive discretion on the part of the controller, the risk of under-reporting or overreaction, and uncertainty in the face of possible inspections or sanctions is particularly critical for SMEs.

Negative comments:

- **Criticism of the single list**: Risk of failure of the current system; suggestion to use the DPIA as a reference tool instead.
- **Nature of the list:** Should not be exhaustive but should instead provide specific evaluation criteria for analyzing risks.
- **Inappropriate review period:** The three-year period is considered far too long given the rapid evolution of digital technologies.

Question 11: Proposal to allow the exceptional use of special categories of data in the context of the development and operation of an AI system or an AI model where appropriate safeguards are in place.

Quantitative results:



Positive comments:

- **Combating bias:** The "bias detection" aspect is seen as a major added value.
- **Regulatory compliance:** The amendment to the AI Act is fairly well received by respondents.
- **Valorization of sensitive data:** These provisions are considered relevant, particularly in the field of health.
- **Robust safeguards:** The set of safeguards provided for – strict necessity, impossibility of effective alternatives (synthetic or anonymised data), pseudonymisation, access controls, non-transferability, early deletion and traceability – is robust and consistent with the principles of the GDPR.

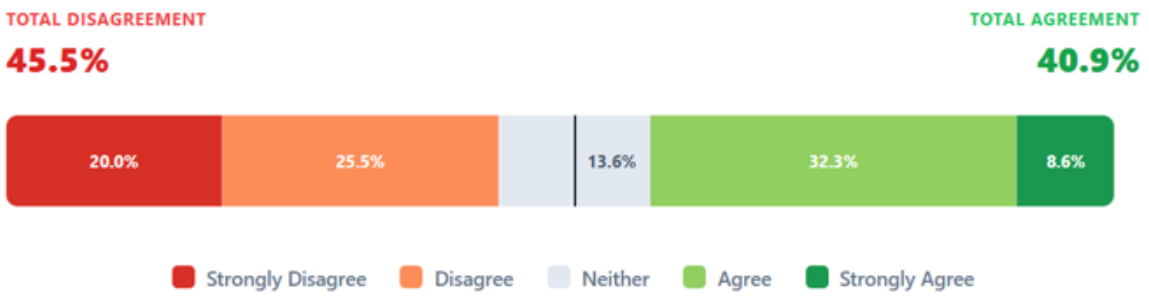
Negative comments:

- **Difficulty of implementation:** The transition to practice is considered complex. DPOs are already overwhelmed by other issues. Leaving the decision on use to the data controller itself may lead to a proliferation of inappropriate uses and that the adoption of preventive and corrective measures may come too late.
- **Lack of control over AI systems:** AI technologies are not yet sufficiently mastered technically. There are real difficulties in applying the right to erasure of data.
- **Technical necessity vs. risk of abuse:** From a technical perspective, the detection and mitigation of biases in high-risk AI systems is not always possible without controlled access to sensitive variables, but there is a risk that this exceptional legal basis will be used beyond the detection and correction of biases or will lead to a normalisation of the use of special categories in AI training.

- **Refusal to amend Article 9 of the GDPR:** Refusal to amend this article, as the additions are considered too broad. The concept of "appropriate measures" is criticized for its lack of precision (too vague).
- **Maintaining the principle of prohibition:** The processing of sensitive data must remain prohibited by default due to its nature. Without explicit consent, there is a risk of loss of security for the individual's rights. The potential dangers and risks for the individuals concerned are considered too significant.
- **Concerns about the lack of protection for data subjects:** Several comments express the view that the proposal leaves citizens more unprotected and could lead to the defencelessness of data subjects with irreparable consequences.
- **Need for clear guidelines for SMEs:** Practical implementation requires clear criteria for "disproportionate effort", documentation and record-keeping templates, guidance from the EDPB and national authorities. Without these guidelines, SMEs may face legal uncertainty and high compliance costs.
- **Recurrent Technical Concern:** A specific technical concern, implicit in several comments, is the disproportionate effort exception for data removal from trained AI models. Given that removing data from a model post-training is technically extremely difficult or impossible in most architectures, this exception risks becoming the rule rather than a genuine last resort, effectively creating a broad carve-out for special category data in AI training datasets.

Question 12: Proposal to allow legitimate interest as a legal ground in the context of AI development and operation, as well as AI models, with appropriate measures and safeguards for the rights and freedoms of the data subject in place.

Quantitative results :



Positive comments:

- **Choice of legal basis:** Legitimate interest is the most appropriate legal basis for some.
- **Clarification vs. redundancy:** Numerous AI developments already refer to Article 6.1.f GDPR. The proposal provides legal certainty by explicitly recognising this possibility in the context of AI, although some consider the article redundant since Article 6.1 f) GDPR already exists.
- **Relevant safeguards:** The safeguards provided for are particularly appropriate: strict minimisation from the selection of sources and during training, measures against residual data retention in AI models, reinforcement of transparency, and an unconditional right to object.

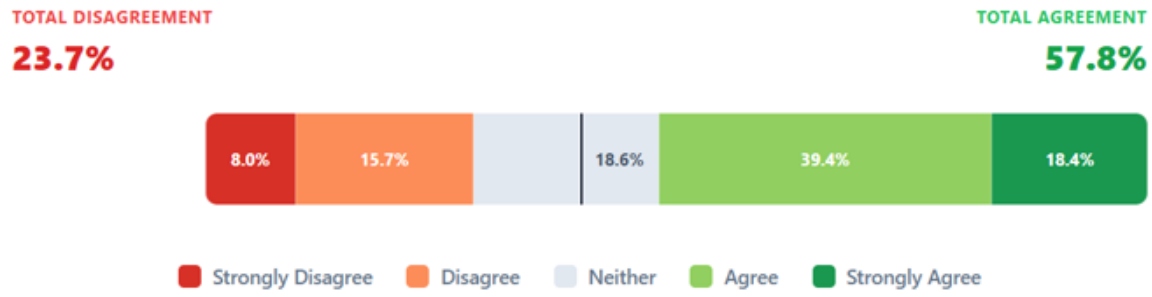
Negative comments:

- **Incompatibility with legal basis:** Rejection of legitimate interest, as AI is considered too intrusive.
- **Risks and lack of trust:** Fear of abuse and processing to the detriment of individuals. Technical and organizational measures are not considered credible in ensuring security.
- **Complexity in terms of individual rights:** The unconditional right to object is considered too complicated to apply, and the provision of information to data subjects raises questions.
- **Need for clarity**: The proposed amendment lacks precision and needs to be clarified. It is suggested that cases should be duly assessed and that additional safeguards should be required beyond simple legitimate interest.
- **Risk of expansive use:** There is a risk that this legal basis will be used as a "default" basis for AI developments, unduly replacing other more appropriate bases (consent, legal obligation), or applied without real and documented consideration. In high-risk systems, legitimate interest should be interpreted restrictively and exceptionally.

Need for guidance for SMEs: For innovative SMEs, this proposal may facilitate the development of viable AI solutions and reduce unnecessary legal barriers, but only if accompanied by clear guidance from the EDPB, AI-specific LIA models, and harmonised supervisory criteria.

Question 13: Proposal to allow the use of biometric data for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.

Quantitative results:



Positive comments:

- **Differentiation between identification and verification:** The proposal is correct in limiting use to verification (1:1) and not identification (1:N). This distinction is essential from the perspective of proportionality and significantly reduces the risks of mass surveillance or improper secondary uses.
- **Exclusive control as a key safeguard:** Requiring that biometric data or means of verification remain under the exclusive control of the data subject introduces a relevant material guarantee, in line with privacy by design approaches and decentralised architectures. However, some comment that exclusive control is equivalent in practice to express consent, and others consider that this exclusive control cannot be guaranteed.

Practical utility for digital services and SMEs: In contexts of strong authentication, fraud prevention, and secure access to digital services, this legal basis can facilitate effective solutions without resorting to centralised biometric repositories, reducing risks and compliance costs for SMEs.

Negative comments:

- **Insufficient control:** The control exercised by the data subject is considered too weak to guarantee data security and protect their rights and freedoms.**Risk of marginalization:** There is a fear that this control will become merely incidental (secondary) over time.
- **Need for technical clarity:** The proposal is unclear and requires clarification on the specific means made available to individuals to exercise this control. The concept of

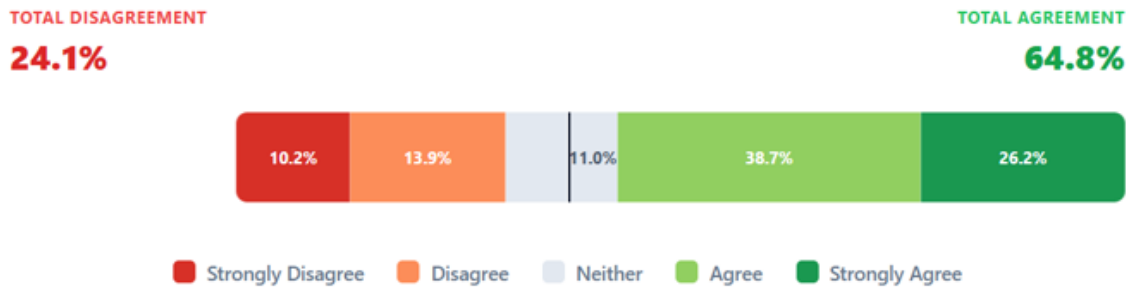
exclusive control must be interpreted strictly and verifiably: no copies on the controller's servers, no indirect or persistent access, no reuse for other purposes.

- **Need for additional guarantees:** To avoid undue standardisation of biometric use, it would be desirable to reinforce genuine voluntariness (equivalent non-biometric alternatives), strict purpose limitation, non-retention by the controller, and impact assessments where appropriate.
- **Concerns about irrecoverable consequences:** Once the confidentiality of biometric data has been breached, the consequences are irrecoverable for the data subject, calling into question the advisability of allowing its use.

Confusion about applicable article: Several comments point to confusion about whether the amendment refers to Article 10 or Article 9.2 of the GDPR.

Question 14. Proposal to give data controllers the possibility to charge a fee or refuse to act on requests when it is deemed that data subjects are abusing the rights provided by the GDPR for purposes other than data protection.

Quantitative results:



Positive comments:

- **Combating abuses:** Combating abusive requests is considered legitimate, as the exercise of the right of access is often misused.
- **Corrects a prejudice against the data controller**: Requests are sometimes used to build litigation cases at no cost, which undermines the data controller's right to evidence.
- **The issue of scope appears to have been resolved:** The proliferation of requests for all emails or collaborative tools is unmanageable for companies, as they are unable to restrict the scope of searches.
- **Clarification of existing powers:** Article 12.5 of the GDPR already covers requests that are "manifestly unfounded or excessive". The proposal does not introduce a new right,

but clarifies a particularly problematic scenario in practice: the abuse of rights for purposes other than data protection.

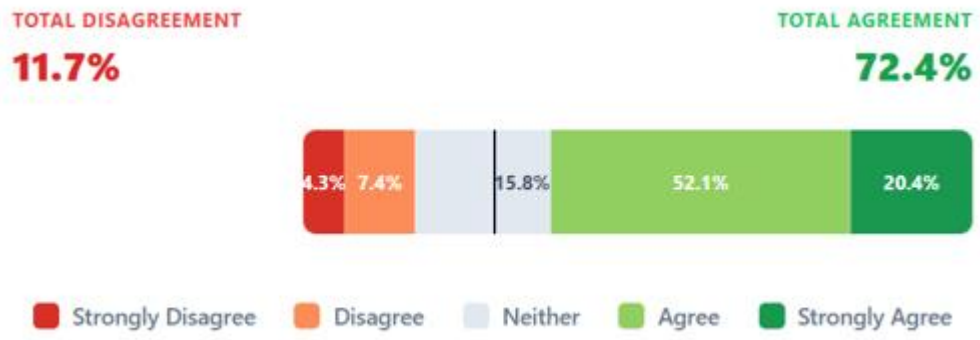
- **Necessary protection for SMEs:** Massive, repetitive or instrumentalised requests generate disproportionate administrative costs. The possibility of a reasonable fee or reasoned refusal contributes to the sustainability of compliance without emptying the rights of data subjects of their content.

Negative comments:

- **Uselessness and fear of abuse:** The current legal framework is considered sufficient. There is a fear that companies will abuse the system by repeatedly claiming compensation.
- **Refusal to limit rights:** Opposition to the ability to refuse to comply with a request to exercise a right.
- **Need for legal clarity:** There is a need to precisely define excessive requests and unfounded requests.
- **Risk of a deterrent effect:** There is a risk that an expansive interpretation may deter the legitimate exercise of rights, disproportionately affect vulnerable groups, or be used as an automatic defence mechanism. Therefore, the notion of "purposes other than data protection" must be interpreted restrictively and with objective criteria.
- **Operational impact:** This measure risks further complicating the role of the DPO.
- **Guarantees and supervision**: Need to estimate costs in advance and set up an external appeal mechanism (such as an authority) to challenge refusals or unjustified costs. It is essential to maintain the burden of proof on the controller, the written reasoning for the decision and the possibility of appeal to the supervisory authority. These guarantees prevent arbitrary decisions.
- **Need for harmonised guidance from the EDPB, instead of modifying the GDPR:** For uniform application across the EU, EDPB guidelines with clear examples of abuse, criteria for calculating the reasonable fee, and standards of justification are essential. This is particularly relevant for SMEs.

Question 15: Proposal on the burden of demonstrating that a data subject's request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.

Quantitative results:



Positive comments:

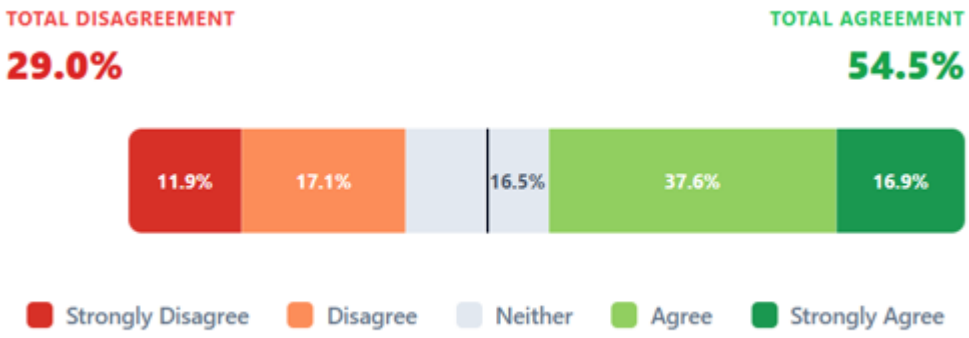
- **Consistency with the principle of proactive responsibility:** The GDPR is based on the controller demonstrating compliance and justifying their decisions. Placing the burden of proof on the controller in this case is a logical consequence of Article 5.2 of the GDPR and avoids defensive interpretations that unduly shift the burden to the data subject.
- **Prevention of arbitrary decisions:** Without this express clarification, there is a risk that controllers will automatically or generically classify certain requests as abusive. Requiring documented evidence reinforces individualised reasoning, improves the traceability of the decision and facilitates control by the authorities.
- **Protection of the essential core of rights:** The rights of access, rectification, erasure and objection are fundamental rights. The burden of proof on the controller acts as a structural guarantee against possible undue restrictions.
- **Legal certainty for SMEs:** Although this may seem like an additional requirement, in practice it benefits diligent SMEs, as it clarifies the standard of proof required, reduces the risk of penalties for ill-founded decisions and encourages clear and defensible internal procedures
- **Alignment with current practice:** Many supervisory authorities already require the controller to provide solid justification for classifying a request as unfounded or excessive. The proposal brings harmonisation and predictability at European level

Negative comments:

- **Weakening of rights and risk of abuse:** The measure is perceived as a setback for individual rights and raises concerns about bad faith and abuse by data controllers.
- **Need for legal clarity:** There is a need to precisely define excessive requests and unfounded requests. Also, there is a need for unified criteria; the lack of unified criteria will render this provision meaningless.
- **Procedural shortcomings:** The measure is considered insufficient. Questions arise regarding the burden of proof, and suggestions are made to establish external appeal mechanisms.
- **Operational impact:** The implementation of these rules may create new practical difficulties for the DPO.

Question 16: Proposal to reduce the amount of information that needs to be given to data subjects only in the context of directly collected personal data in low-risk, non-intensive processing scenarios, specifically when there's no external sharing or international transfer, no automated decision-making, and the data subject is reasonably presumed to be already informed.

Quantitative results:



Positive comments:

- **Agreement with the principle, reservations about the wording:** The basic idea is considered good, the central objective being to avoid overwhelming the user. Technical

transfers with no real implications (e.g., hosting in the EU) should not be an obstacle to simplifying the information. However, the current wording of the proposal needs to be revised.

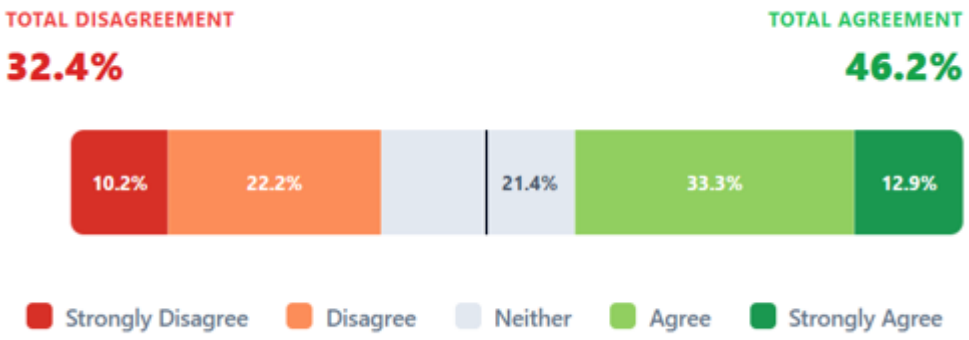
- **Improved readability:** Adapting information according to the level of risk and the simplicity of processing is seen as a positive lever for making information clearer.
- **Strict delimitation of scope:** It is positive that the exception is automatically excluded when there are external recipients, international transfers, automated decision-making or profiling, or the processing may involve high risk. This delimitation reduces the risk of abusive use of the exception.
- **Usefulness for SMEs:** For SMEs and micro-enterprises with simple and stable processing, the proposal may reduce redundant administrative burdens, promote more understandable and realistic compliance, and avoid "information fatigue" on the part of the data subject.

Negative comments:

- **Criticism of the wording and lack of objectivity:** The wording is considered too subjective. There is a demand for objective criteria to define vague concepts such as “clear and circumscribed relationship,” “not date-intensive,” or “reasonable grounds.”
- **Concerns about the concept of "reasonable grounds":** The presumption that the data subject already has the information should be interpreted in a restrictive and verifiable manner, and not as an automatic exemption. The controller must be able to demonstrate this circumstance. Clarity is required on what these reasonable grounds are.
- **Infringement of rights and transparency:** The measure is perceived as weakening individuals' rights and undermining the principle of transparency, solely for the benefit of data controllers.
- **Practical inapplicability:** Some believe that, in its current form, this exemption will never be applied. Rewording is necessary to truly simplify the mechanism.
- **Need for additional safeguards:** It would be advisable to keep at least a minimum amount of essential information accessible (identity of the controller and purpose), to ensure that complete information is permanently available on request, and to provide simple mechanisms for accessing such information.

Question 17. Proposal to reduce the amount of information to be given to data subjects when their personal data is collected directly for processing in the context of scientific research purposes, where providing notice is impossible or would impair research.

Quantitative results:



Positive comments:

- **Non-commercial use condition:** Acceptance of the text should be reserved exclusively for non-commercial purposes.
- **Alignment with the Article 89 GDPR framework:** The GDPR recognises that scientific research poses structural tensions with certain procedural principles, including comprehensive individualised information. The proposal fits correctly within this framework, without creating an autonomous exemption.
- **Safeguards and conditions:** It is positive that the exception is conditional on: impossibility or disproportionate effort duly justified, real risk to the objectives of the research, application of enhanced safeguards in accordance with Article 89.1, and the obligation to take alternative measures, including public disclosure.

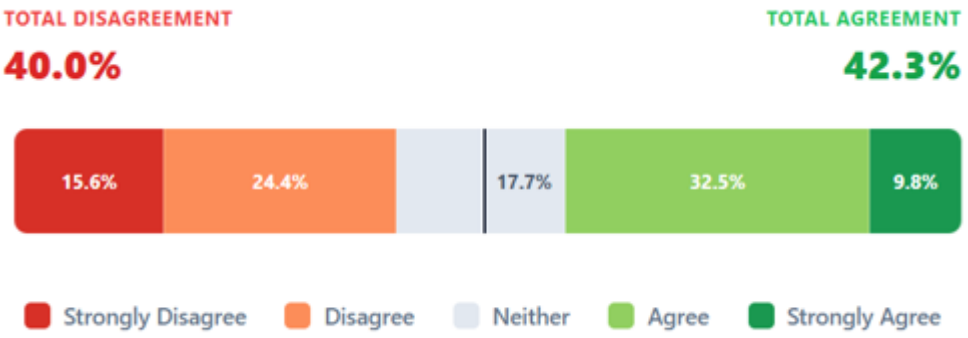
Negative comments:

- **Opposition to the commercial framework:** The text is considered too open to interpretation and requires clarification to firmly exclude any commercial research.
- **Requirement for legal precision:** Requests for clarification have been made regarding the definition of "impossible" referred to in the article.
- **Primacy of individual rights:** Some argue that the interests of individuals must take precedence over research, stating that the GDPR must apply to everyone without distinction so as not to weaken rights.

- **Risk to transparency:** The measure is perceived as an infringement of the principle of transparency, as individuals must be kept informed regardless of the context.
- **Proposal for sectoral restriction:** It is suggested that the application of these exemptions be limited solely to the field of medical research.
- **Sensitivity with special data:** In research involving special categories of data, biometric data or neurodata, the reduction of information must be applied with increased caution, prior DPIA where appropriate and independent ethical control. It is stated that undermining the right to information will be detrimental to the data subject when special categories of data are processed.

Question 18: Proposal to simplify Article 22 of the GDPR regarding automated decision-making.

Quantitative results:



Positive comments:

- **Simplified wording:** The measure is welcomed for its ability to make the wording simpler and more accessible.
- **Pragmatic approach:** The text is seen as a concrete solution that is adapted to the realities on the ground.
- **Extension subject to no opposition:** It is suggested that the measure should be made possible as long as the person is clearly informed and has not expressed any opposition.

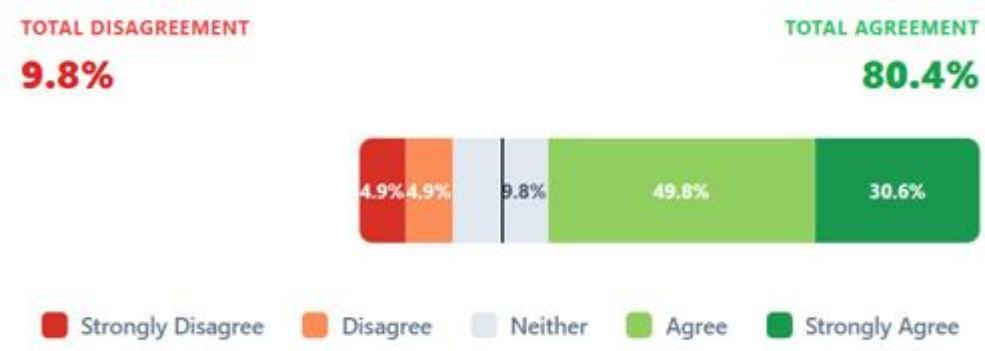
Negative comments:

- **Deregulation vs. simplification:** The proposal is perceived not as a simplification but as a deregulation that nullifies the right not to be subject to automated decisions.

- **Risk of misuse and inadequate legal basis:** The exception related to contractual necessity risks being used extensively without any real test of necessity; legitimate interest would be preferable to impose a systematic balancing of interests**.**
- **Elimination of material safeguards:** The current wording of Article 22 not only lists the enabling bases, but also limits the "solely automated" nature, requires additional safeguards (human intervention, right to challenge, right to express one's point of view), and is articulated with recitals 71 and 75. The new proposal reduces the article to an enabling clause, implicitly shifting essential safeguards to other provisions.
- **Lack of safeguards for automated processing:** The use of automated processing presents too many risks for individuals and lacks safeguards for control.
- **Legal and drafting inaccuracies:** The wording needs to be reviewed, in particular to clarify whether the conditions are cumulative or alternative, and the reference to EU Member States is causing disagreement.
- **Exploitation of biases and lack of fairness:** The technical impossibility of guaranteeing the fairness of algorithms raises fears of the exploitation of discriminatory biases; human intervention should be required for any decision producing legal effects.
- **Negative impact on the protection of rights:** The proposed simplification weakens the data subject's control over decisions that significantly affect them, the requirement for explainability and review, and the ability to effectively challenge decisions. From a fundamental rights perspective, this regression is difficult to justify.
- **Inconsistency with the AI Act:** The AI Act reinforces human oversight in high-risk systems. Simplifying Article 22 of the GDPR in a permissive sense creates regulatory dissonance between data protection and AI governance.
- **Risk for SMEs:** Although the proposal may appear to be an operational facilitation, in practice it may increase litigation, generate legal uncertainty due to divergent interpretations, and expose controllers to conflicts with authorities and courts. Clear protection is, in the long term, safer than excessive simplification.
- **Need for a more balanced alternative:** It would be preferable to clarify concepts such as "significant human intervention", harmonise Article 22 with the AI Law, and strengthen interpretative guidelines, without emptying the substantive guarantees of the provision of their content.

Question 19. Proposal to empower the Commission with the competence to adopt a list of processing operations which are subject to the requirement for a DPIA and a list of the kind of processing operations which are not subject to the requirement for a DPIA on the basis of lists proposed by the EDPB.

Quantitative results:



Positive comments:

- **Positive reception of harmonization:** The initiative to harmonize practices has been well received, as the current national lists have led to significant divergences between Member States, legal uncertainty for organisations operating in several countries, and particular complexity for SMEs and digital start-ups.
- **Strengthening legal certainty:** The development of lists and a common methodology at the European level is seen as a step forward in terms of consistency of practices and legal certainty.
- **Institutional balance:** The proposed model is considered legally sound, with the EDPB providing technical, supervisory and practical expertise, and the Commission ensuring regulatory consistency and formal adoption through implementing acts, respecting the institutional balance and reinforcing the legitimacy of the outcome.
- **Ex ante clarity on obligations:** Having a positive list (mandatory DPIA) and a negative list (DPIA not required) drastically reduces interpretative uncertainty and avoids both defensive over-compliance and risk underestimation.
- **Common methodology for quality:** A harmonised methodology improves the technical quality of DPIA, facilitates their review by authorities, reduces compliance costs, and professionalises risk management in data protection, especially in SMEs.
- **Periodic update:** Mandatory review every three years is considered essential in an environment marked by AI, big data, biometrics, neurotechnologies, and emerging

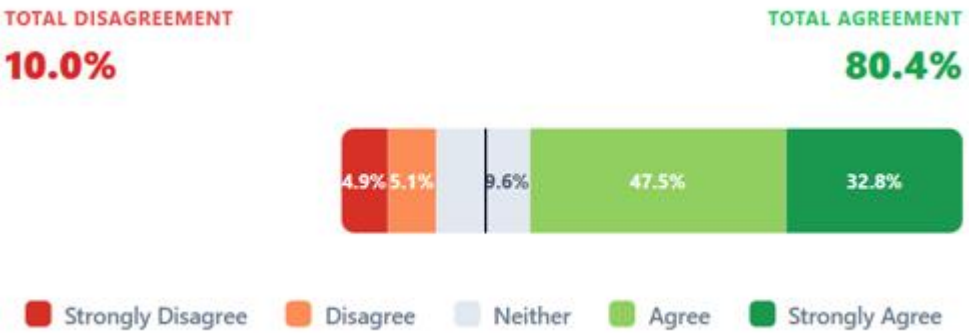
systems, preventing lists and methodologies from becoming obsolete, although some participants consider this timeframe to be excessively long.

Negative comments :

- **Inadequacy in practice:** There is concern that establishing an exhaustive list may not correspond to the operational realities on the ground.
- **Challenge to centralization:** The rigidity of the list is questioned; it is suggested that this power be left to local supervisory authorities, or that they be included in the process, or that centralization be limited to the EDPB.
- **Excessive review period:** The three-year period for reviewing the list is considered too long in view of changing needs.
- **Risks of inaction and inflexibility:** The measure risks weakening the responsiveness of local authorities, making the accountability process more rigid, and imposing single models that are unsuited to specific sectors.
- **Security concerns:** Concerns have been expressed about the potential negative impact of this measure on data security.

Question 20. Proposal to empower the Commission with the competence to adopt a common template and methodology for conducting DPIAs based on drafts proposed by the EDPB.

Quantitative results:



Positive comments:

- **Usefulness of harmonization**: The measure is seen as useful for improving the quality and consistency of practices, while also helping SMEs.

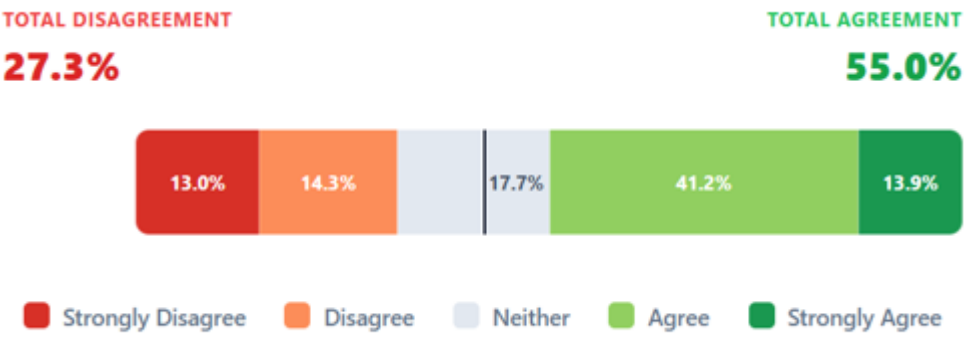
- **Legal and operational progress:** The initiative is considered a major step forward in terms of consistency, clarity, and legal certainty.
- **Positive impact for SMEs:** DPIAs are one of the most complex instruments in the GDPR. Having a clear template and a structured methodology facilitates compliance for SMEs, start-ups and entities with limited resources, reducing costs and errors.
- **Improving supervisory effectiveness:** Comparable and structured DPIA enable authorities to assess risks more quickly, identify recurring deficiencies and better guide those responsible.
- **Technological update:** Review at least every three years is essential in a rapidly evolving technological environment, avoiding obsolete methodologies in the face of AI, biometrics or emerging treatments.

Negative comments:

- **Request for priority to supervisory authorities:** It is suggested that the EDPB and national supervisory authorities be responsible for framing this issue rather than a central authority.
- **Preservation of existing analyses:** Acceptance is conditional on there being no impact on DPIA already carried out according to current methodologies, with subsequent revisions then being aligned with the new model.
- **Adequacy of national frameworks**: The national regime already in place is considered sufficient.
- **Mistrust of the Commission's role:** The attribution of this competence to the European Commission raises many questions.
- **Methodological freedom:** It is suggested that data controllers and DPOs be given a free choice of working methodology.
- **Conceptual confusion in existing guidelines:** It is noted that some national guidelines have confused fundamental concepts such as risk factor and risk leading to legal uncertainty and inconsistent implementation among Member States.

Question 21. Proposal to reduce obligations by introducing provisions regarding cookies and similar technologies that are storing personal data or gaining access to personal data already stored in the terminal equipment of a natural person in the GDPR.

Quantitative results:



Positive comments:

- **Regulatory clarity and reduction of fragmentation :** Unifying the rules regarding cookies in the GDPR improves legal certainty and reduces confusion arising from the overlap between ePrivacy and the GDPR, which is particularly beneficial for SMEs that currently face divergent interpretations and complex technical solutions**.**
- **Regulation of the frequency of consent requests:** The introduction of a time limit between two consent requests is considered positive to prevent users from being asked for consent too often or too quickly.
- **Approval of storage methods:** The provisions of paragraph 4 concerning new data storage methods have been well received.
- **Exceptions consistent with practice:** The proposed exceptions (transmission of communications, requested service, own audience measurement and security) are aligned with established criteria and avoid unnecessary burdens when there is no relevant impact on rights.

Negative comments:

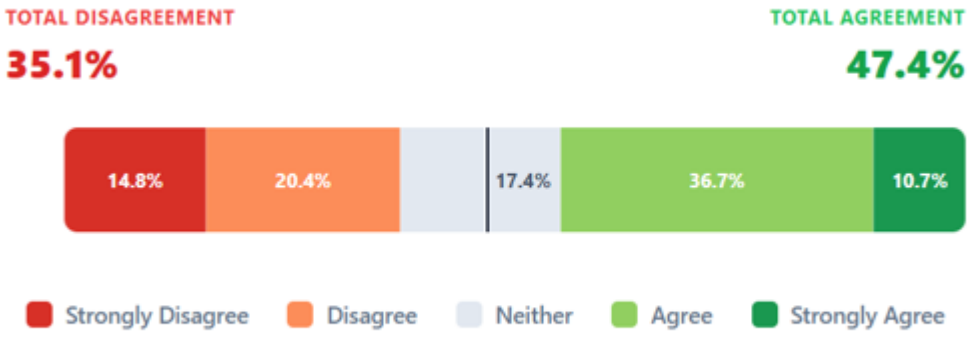
- **Increased complexity and lack of transparency:** The proposal is seen as a source of additional complexity. The requirement for transparency must remain a top priority.
- **Major textual inaccuracies:** The text lacks clarity on critical points, including the identification of the data controller, the procedures for withdrawing consent, and the absence of any mention of retention periods. It will be essential to clearly define

concepts such as "audience measurement for own use" and "expressly requested service" and to harmonise technical criteria (local storage, SDKs, non-cookie technologies).

- **Suspicion of lobbying and regression:** The proposal is perceived as reducing the scope of consent, and there are fears that this may be dictated by lobbying interests. It is suggested that the current system be tightened up before new provisions are added.
- **Risk of consolidating a consent-centred model:** There is concern that the proposal reaffirms consent as the cornerstone even in scenarios where other legal bases might be more appropriate, which may perpetuate operational friction and "bannerisation" practices with no real informational value.
- **Privacy concerns:** Some participants express outright rejection of spying through cookies, pixels, or any similar technology.

Question 22: Proposal to reduce the necessity for consent where the analysis is conducted by the data controller.

Quantitative results:



Positive comments:

- **Consistency with the principle of proportionality:** Basic audience analytics, limited to own use, for statistical purposes and without significant impact on the rights of the data subject, presents a low risk, especially when it does not involve profiling or cross-site tracking.
- **Benefit for SMEs:** For SMEs, e-commerce businesses and entrepreneurial projects, this exception reduces dependence on intrusive banners, provides insight into the basic functioning of the service and reduces disproportionate technical and legal burdens.

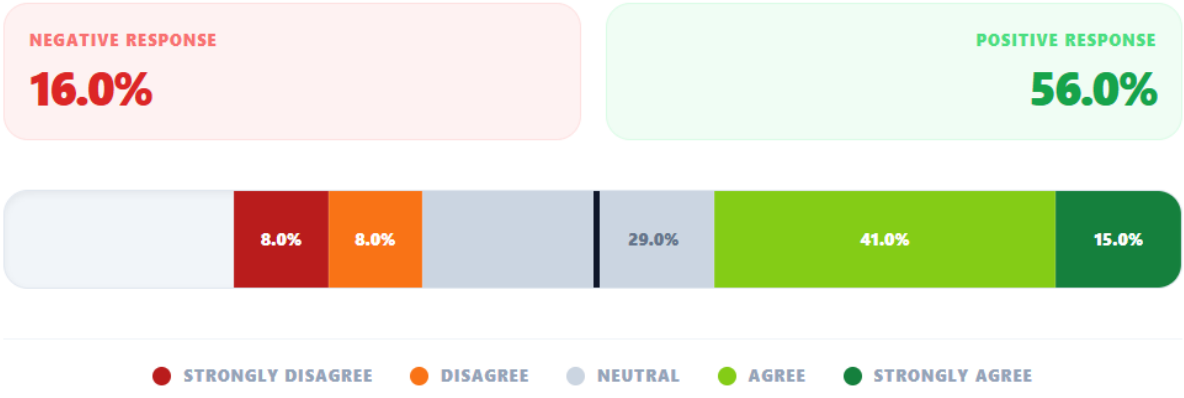
- **Need for strict interpretation:** Support for the proposal is conditional on ensuring exclusively internal use without third parties or transfers, aggregated and non-identifying data, no profiling, cross-site tracking or reuse, short retention periods and minimisation measures.

Negative comments:

- **Risk of misuse and abuse:** The proposal is perceived as a potential lever enabling data controllers to unduly exempt themselves from the obligation to obtain consent.
- **Risk of Functional Expansion :** Without a precise definition of "audience measurement" and "own use," there is a risk that third-party SDKs will be integrated, expanded to advanced analytics or advertising, or that tracking will be reintroduced under a statistical label. This requires clear guidelines and effective controls.
- **Inconsistency and threat to privacy:** The mechanism is considered inconsistent and a direct threat to privacy. The requirement to provide information on the use of data must remain universal.
- **Weakening of individual control:** There is serious concern about the loss of transparency and control for users over their own personal data.
- **Imbalance of rights:** This development risks favoring the interests of data controllers at the expense of the legitimate expectations of users, particularly in digital public services.

Question 23. Proposal to require online interfaces and browsers to support machine-readable consent mechanisms.

Quantitative results:



Positive comments:

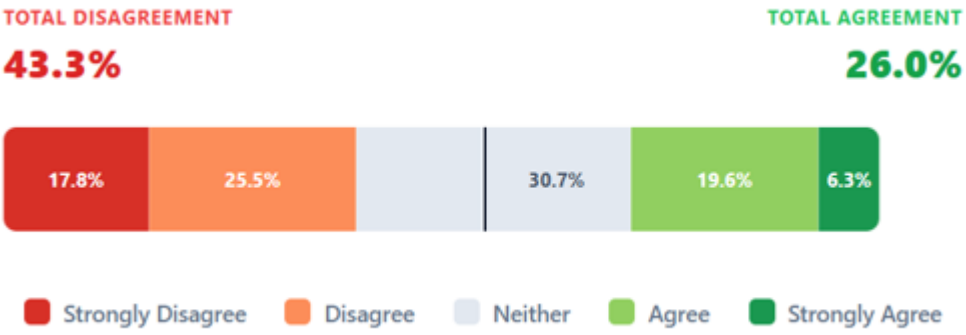
- **Combating consent fatigue and dark patterns:** The requirement for machine-readable mechanisms is welcomed as a positive development. It strengthens the effectiveness of people's choices while promoting harmonization within the EU.
- **Consistency with technical developments:** The mandate to European standardisation bodies and the presumption of conformity for interfaces aligned with harmonised standards is a legally sound solution that avoids imposing rigid technical specifications in the legal text and promotes interoperability.
- **Proportional design for SMEs:** It is appropriate to exclude media service providers in their editorial function, defer implementation (24 and 48 months), and limit the direct obligation to browser providers that are not SMEs, mitigating disproportionate impacts and facilitating progressive adoption.

Negative comments:

- **Concerns about deadlines and wording :** Some participants consider that the deadlines for implementation (24 and 48 months) are too long and that the wording could be improved**.**
- **Doubts about operational and technical feasibility:** Practical implementation is considered impossible. The concept of "supporting machine-readable consent mechanisms" is criticized for its lack of clarity.
- **Economic and industrial risks:** The application of this article could have a significant impact on CMP providers and suppliers.
- **Opposition to the exclusion of SMEs:** the rules should apply to all companies, regardless of their size.
- **Requirement for increased transparency:** Simplification must not result in a loss of control. It is imperative that internet users be able to understand the scope, range, and lifespan of each tracker, while also having access to the information that is actually collected.
- **Implementation and technical governance risks:** There is caution about the quality and neutrality of the standards to be developed, preventing browsers from becoming gatekeepers of consent, and ensuring that machine-readable signals do not replace clear and accessible information when necessary. Transparent governance of the standardisation process and interpretative guidelines from the EDPB will be key.
- **Need for additional safeguards:** For a guarantee-based implementation, the traceability and auditability of signals, simple revocation mechanisms, compatibility with explicit consent when required by the GDPR, and protection against unwanted default settings must be ensured.

Question 24. Proposal to exempt media service providers from the requirement to provide online interfaces and browsers to support machine-readable consent mechanisms.

Quantitative results:



Positive comments:

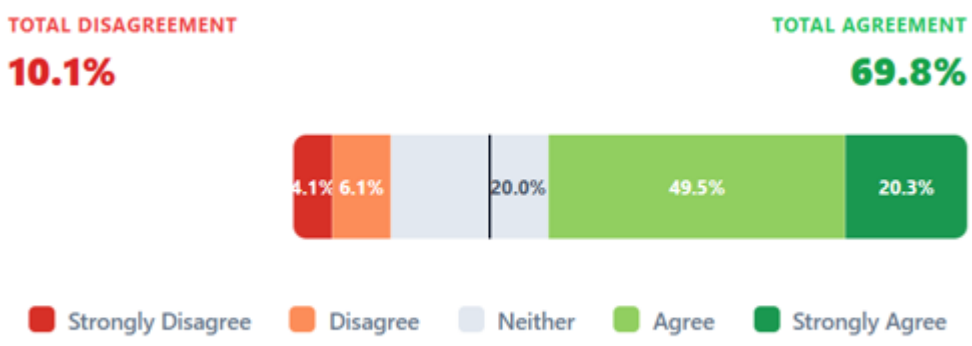
- **Protection of freedom of information and media pluralism:** Media services fulfil a specific constitutional and European function. Imposing technical obligations designed for digital tracking and monetisation environments could unduly interfere with editorial freedom and legitimate funding models, especially in small and local media.
- **Consistency with the EMFA Framework:** The exemption is consistent with the logic of Regulation (EU) 2024/1083 (European Media Freedom Regulation), which recognises the unique nature of the sector and the need for specific safeguards against disproportionate technical burdens that could affect editorial independence.
- **Technical and economic proportionality:** The implementation of machine-readable signals requires technical and interoperability capabilities that not all media outlets, particularly SMEs and regional media, can assume without significant impact. The exemption avoids a crowding-out effect from the information market.
- **Necessity of the provision:** The adoption of these mechanisms is considered essential.
- **Effectiveness of the exemption:** The implementation of machine-readable mechanisms is seen as a concrete step forward in ensuring that users' decisions are respected while reducing the fatigue associated with repeated requests. This approach promotes greater consistency between interfaces, browsers, and online services, while remaining aligned with the principles of the GDPR (free and informed consent).

Negative comments:

- **Categorical rejection of media exemption:** The proposal to exempt media service providers is firmly rejected. The exception is considered dangerous because it could encourage entities to misuse the status of “media” to exempt themselves from regulation to the detriment of users.
- **Lack of objective justification:** No valid technical or legal reason has been identified for this exception.
- **Institutionalization of unequal treatment:** This measure is considered incompatible with the fundamental principles of the GDPR.
- **Need for clarification or deletion:** If the exception were to be retained, it is requested that its scope be strictly limited (use of the term “exclusively”). However, the prevailing position remains that it should be deleted outright to ensure a unified and enforceable consent signal.
- **Primacy of transparency:** It is strongly reiterated that simplification must not under any circumstances justify a loss of transparency or control over personal data.
- **Need for strict delimitation:** The exemption should apply only when the controller provides a media service in the strict sense; it should not extend to ancillary activities (behavioural advertising, adtech, data brokerage) or to platforms that self-classify as "media" without meeting the substantive criteria of the EMFA. Material delimitation is key to avoiding regulatory arbitrage.

Question 25: Proposal to require web browsers to provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object.

Quantitative results:



Positive comments:

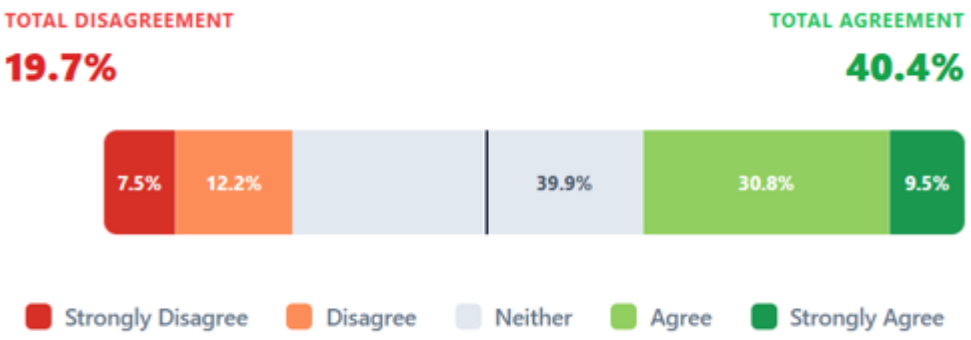
- **Support for browser obligations:** Support is expressed for the obligation on browsers to incorporate automated, machine-readable consent mechanisms.
- **Strengthening the effectiveness of rights:** This proposal is welcomed as a major lever for ensuring that consent, refusal, and the right to object can be expressed by equivalent means. It actively contributes to the fight against misleading interfaces (dark patterns) and improves the portability of privacy choices.
- **Proportional burden sharing:** It is appropriate to limit the obligation to browser providers that are not SMEs and to set generous implementation deadlines (24/48 months). This avoids disproportionate impacts and allows for orderly technical adoption.
- **Standardisation and interoperability:** The use of harmonised standards requested by the Commission favours interoperable solutions and avoids fixing specific technologies in law. The presumption of conformity encourages adoption and legal certainty.
- **Improved compliance for controllers:** Machine-readable signals reduce friction and facilitate uniform respect for user preferences, with clear operational benefits for SMEs and digital services.

Negatives comments:

- **Need for standardization:** The implementation of automated and machine-readable choices is considered technically impossible without the establishment of common and universal standards**.**
- **Priority given to clarity of information:** Automation must not in any way obscure the obligation to provide clear prior information, which remains an essential condition for valid consent.
- **Independent technical governance:** It is imperative that the establishment of standards be entrusted to recognized technical entities, rather than to the European Commission or data controllers, to avoid biased standards.
- **Risk of browsers as gatekeepers:** Caution is needed to prevent browsers from becoming gatekeepers of consent. It is essential to ensure neutrality in interfaces and default values, transparency and auditability of signals, easy revocation and user control, and compatibility with explicit consent where required by the GDPR.

Question 26. Proposal to maintain article 5(3) in the ePrivacy directive regarding cookies and similar technologies and specifying that it shall not apply if the subscriber or user is a natural person, and the information stored or accessed constitutes or leads to the processing of personal data.

Quantitative results:



Positive comments:

- **Consistency of the text**: Overall, the measure is considered structurally consistent.
- **Clarification of the relationship between ePrivacy and the GDPR:** This clarification is welcomed as it usefully clarifies the link between the ePrivacy Directive and the GDPR. It ensures that the processing of personal data remains fully subject to the requirements of the GDPR, thus avoiding any risk of circumvention through a purely technical qualification.
- **Balanced alternative:** It is proposed to maintain the application of Article 5.3 e-Privacy also when personal data is involved, coordinating it with the GDPR through clear rules of prevalence and harmonised guidelines, preserving protection and providing legal certainty.

Negative comments :

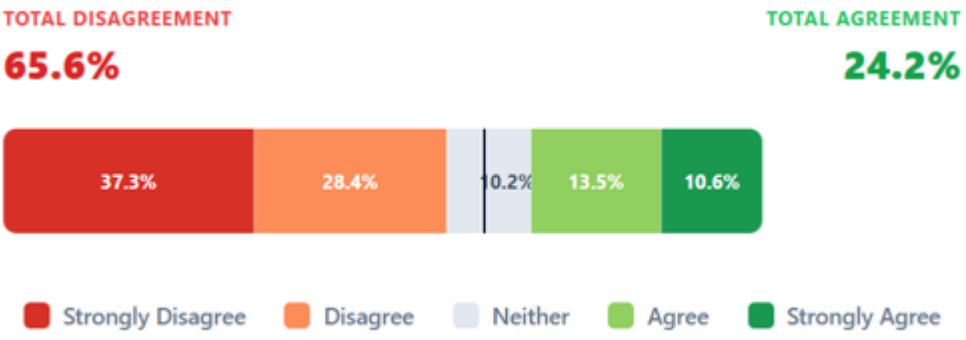
- **Lack of clarity and risk of circumvention:** The text lacks precision, raising concerns that individuals could be used as fronts to circumvent obligations.
- **Risk of instrumentalisation of the ePrivacy/GDPR articulation:** The proposed exception risks exacerbating bad practices by data controllers.
- **Opposition to any hierarchy of texts:** The GDPR and the ePrivacy Directive must remain complementary and distinct, with one regulating access to terminals and the other

regulating data processing after collection. Any attempt at implicit merger or hierarchy is firmly rejected as it would weaken privacy protection.

- **Reduction of protection at the point of entry:** Access/storage on terminal equipment is a technical intrusion prior to the processing of personal data. Replacing this protection with the GDPR shifts control ex post and weakens the ex ante safeguard offered by e-Privacy.
- **Inconsistency with fundamental rights:** The confidentiality of communications and terminal equipment (Article 7 of the Charter) should not be subject to subsequent classification as "personal data". These are distinct and cumulative areas of protection.
- **Adverse impact on SMEs and users:** Far from simplifying matters, the proposal complicates compliance and may erode user confidence by reducing clear guarantees on the use of cookies and similar technologies.

Question 27. Proposal to eliminate the necessity of maintaining a record of processing activities (ROPA) for organizations with less than 750 employees, instead of 250 employees as it is currently, unless the processing is likely to result in high risk to the data subjects.

Quantitative results:



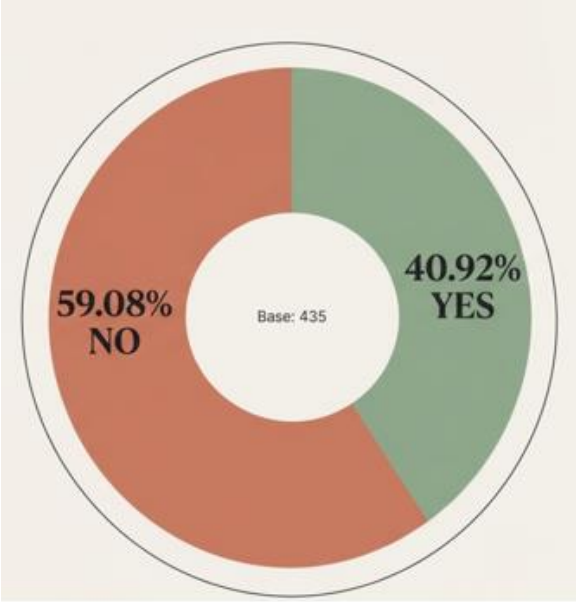
Negative comments :

- **Ambiguity of the concept of high risk:** The exception based on “high risk” is considered far too open to interpretation to be a reliable criterion. Making the obligation conditional only on "high risk" (Art. 35) without a prior ROPA makes it difficult to identify that risk. This creates a paradox: to know if there is high risk, the controller needs a minimum inventory of processing operations. There is no risk analysis without a ROPA.

- **Undermining an essential compliance tool:** The removal of the record-keeping requirement is very unwelcome, as it is an essential management tool, regardless of the size of the company.
- **Obstacle to the work of DPOs and the exercise of rights:** This measure would deprive DPOs of resources and prevent companies below the threshold from responding effectively to requests to exercise individual rights due to a lack of documentation.
- **Suggestion for a simplified ROPA for companies below the threshold:** Rather than removing the ROPA, it is suggested that a simplified template be introduced for small entities to ensure basic compliance.
- **Irrelevance of the workforce criterion:** The number of employees alone is not sufficient to assess the impact of processing; market share, the nature of the services, or a dominant position are considered much more relevant criteria**.**
- **Risk of circumvention strategies:** This measure could encourage large companies to transfer their activities to subsidiaries or partners that meet the exemption criteria to avoid their responsibilities.
- **ROPA as a starting point for compliance:** The ROPA is the necessary starting point for compliance. Without a ROPA, the data being processed, the purpose, and the communications or transfers are not documented. Without the ROPA, it is impossible to assess and control the risks of the entity and the processing operations carried out. It is the basis for everything else, mainly risk assessment.
- **Benefits of the ROPA for SMEs:** SMEs that currently maintain a basic ROPA benefit from better internal management, reduce the risk of penalties, and facilitate audits and DPIA where appropriate. Broad exemption can encourage reactive compliance and hinder supervisory work.
- **Misalignment with other regulatory frameworks:** In a context of regulatory convergence (IA, NIS2, DORA), the documentation of processing operations is a cross-cutting requirement. Lowering the GDPR standard runs counter to this trend.

Question 28: Digital Omnibus will make my role as a DPO more impactful in my organisation.

Quantitative results:



If answered yes:

Comments:

Harmonization and research

Harmonization with NIS 2, ePrivacy, and the AI Act allows the DPO to operate within a consistent global framework. For scientific research, the proposals save time by allowing researchers to focus on critical processing issues.

Role of the DPO and data controller

The measures facilitate certain processes for data controllers, but do not lighten the DPO's workload. Instead, they increase the time needed to monitor and assimilate the rules. Omnibus does not strengthen the DPO's recognition or capacity for action; it impacts their role while increasing legal uncertainty.

Acceptability

The evolution of the framework makes the GDPR more acceptable to stakeholders, creating a win-win dynamic.

Proactive interaction with the data controller

The changes introduced by the Digital Omnibus encourage the DPO to interact more proactively with the data controller.

If answered no:

Comments:

Weakening of status and authority

Regulatory changes are perceived as a sign of "laxity" that undermines the role of the DPO. The freedom to interpret texts and the relaxation of rules risk reducing the authority of the DPO, making them less "audible" to data controllers. For 30% of respondents, other functions could even gain authority at the expense of the DPO on data protection issues.

Loss of substance and missions

Many comments highlight the risk of seeing the GDPR "divested of its essence" through the proliferation of exceptions (AI, media, research) and the abusive use of legitimate interest. The

easing of obligations, particularly the possible removal of the processing register, raises fears of a gradual disappearance of the DPO role in certain structures or its dilution into other functions.

Increased complexity and legal uncertainty

Under the guise of simplification, the proposals are considered to generate complexity and uncertainty. The DPO finds himself increasingly responsible for interpreting vague concepts without having any additional leverage. This situation reinforces his isolation as an expert and complicates his integration from the outset of projects.

Risks to the protection of individuals

The text seems to favour facilitating the use of data rather than protecting rights. This perceived reduction in safeguards (particularly in cases involving sensitive data or large-scale processing) raises concerns about less protection for users and increased difficulties in managing subcontractors.

Redistribution of authority and loss of organisational weight

The most recurring theme among those who perceive a negative impact is that other managers will have more authority than the data protection officer in matters related to data protection. There is criticism that the proposals diminish the DPO's weight in terms of organisational function and undermines fundamental rights..

Reduction of administrative tasks vs. reduction of relevance

There is a dual perception: for those who see a positive impact, the reduction in administrative tasks will allow more attention to be paid to providing practical advice; however, for those who see a negative impact, this reduction in administrative tasks implies less functional relevance for the DPO.

Impact of the new definition of personal data

For those who perceive a negative impact point out that there will be less processing of personal data with the new definition of personal data, which would reduce the scope of action of the DPO.

Legal uncertainty

Respondents identify that there will be more legal uncertainty with the new GDPR and the e-Privacy Directive proposed by the European Commission, which could increase the need for advice from the DPO.

Insufficient resources and more lax regulations

Concern is expressed that it is currently difficult to comply with the obligations of the GDPR and that organisations allocate few resources to the DPO function or to data protection activities;

especially since there is no obligation to carry out audits. Making the regulations more lax will not benefit the protection of the rights and freedoms of individuals.

Less involvement in crisis management

Reduced reporting of security breaches will make the DPO less visible and reduce their participation in crisis committees, diminishing their vertical involvement in the organisation.

Perception of optional compliance

Compliance with the GDPR is already perceived as optional. This reform proposal creates more confusion and less willingness to comply. The DPO and the GDPR often "lose out" when decisions have to be made between several priorities, a trend that will be exacerbated by this reform.

Question 29: Do you think that the GDPR or ePrivacy Directive should be modified in other ways, which are not addressed in the EC's proposals?

Quantitative results:

Comments:

Operational pragmatism and simplification

- Right of access and abuse of rights: Respondents call for pragmatism to be introduced to prevent the right of access from becoming unmanageable in practice, in particular by allowing users to be asked to specify the scope of their request in the event of an exhaustive request.
- Administrative simplification: It is suggested that data breach notification forms be simplified and that the formalities of impact assessments (DPIA) be reduced, as they are considered too burdensome given the pace of projects.
- Thresholds adapted to SMEs: Rather than thresholds based on the number of employees, an approach based on sector or volume of people concerned is recommended to reduce the burden of record keeping.

Clarification and legal harmonization

- Links between texts: Greater consolidation or harmonization is desired between the GDPR and other regulations (NIS 2, DORA, ePrivacy) to avoid inconsistencies, particularly regarding notification deadlines.
- Definitions and transfers: DPOs are calling for clearer definitions (particularly of personal and anonymous data) and a simplification of the mechanisms for transfers outside the EU, which are considered too theoretical.

Governance and missions of the authorities

- Role of supervisory authorities: It is proposed that supervisory authorities alongside the EDPB provide common criteria, decision trees, and clear positions on topics such as cookies and retention periods.
- Sanctions and controls: Professionals want more proportionate sanctions and a more relaxed approach to controls.

Strengthening the status of the DPO

- Independence and resources: Feedback emphasizes the need to ensure that the DPO reports to executive management and is given the real resources to carry out their role rather than simply performing administrative tasks.

New technological challenges

- AI and vulnerability: The framework should better integrate artificial intelligence and strengthen the protection of vulnerable individuals or the data of deceased individuals.

Regulation of emerging issues and regulatory gaps

- Taking into account the years that the GDPR has been in force, certain regulatory gaps have been identified, such as the issue of minors, scraping, surveillance, the use of biometrics, research purposes, and information relating to harassment procedures. Current issues should be addressed and those that have given rise to uncertainty in their application or discrepancies between supervisory authorities should be developed.

International data transfers

- The current regulation of international transfers should be reviewed so that companies do not suffer from political uncertainty and the current bureaucratic burden.

Simplification and practical guidance for compliance

- There should be much more simplification, and there should be more information and guidance from the EC and EDPB to enable more realistic compliance. There should also

be a greater focus on sectors and their specific characteristics. This should be complemented by the existence of more compliance templates generated by the EDPB to standardise how legislation is interpreted across the EU. Provide templates or models from other impact assessments such as TIAs or LIAs.

Inferences, derived profiles and AI

- It would be advisable to clarify the legal status of inferences and derived profiles. The GDPR should expressly address the legal status of inferences (including those generated by AI), especially when they reveal sensitive attributes not directly collected, reinforcing obligations of transparency and risk assessment. Greater attention should be paid to the training, use and results of AI in areas that may affect people's rights.

Regulatory coordination and integration of regulatory frameworks

- Effective regulatory coordination between the GDPR, AI Act, NIS2 and eIDAS is necessary, with an integrated governance framework that avoids overlaps, contradictions and duplicate burdens, with clear criteria for prevalence and coordinated procedures (DPIA, incident reporting, supervision). Harmonisation with the AI Act, the Data Act and the Data Governance Act. Development of a map that allows organisations to identify that if they comply with requirement X of the GDPR, they also comply with requirement Y of the AI Act: Integration of GDPR and AI Act impact assessments.

Specific regulation of biometric data and neurodata

- Enhanced safeguards should be specified for non-invasive consumer biometrics and neurodata, including limits on reuse, strict minimisation rules and privacy by design standards.

Improvement of the automated decision-making regime

- Article 22 should be clarified (not weakened), defining meaningful human intervention, effective rights of explanation, and consistency with the human oversight requirements of the AI Act.

Tools and support for SMEs

- Rather than new exemptions, harmonised tools (templates, methodologies, binding technical guidelines) and uniform criteria are needed to reduce legal uncertainty for SMEs. Greater simplification of administrative requirements and data controller obligations, which hamper their competitiveness.
- Establish well-described minimum measures for security measures in low-impact processing, obligation to establish very clear guidelines by the EDPB and supervisory

authorities with very clear criteria on the minimum requirements for SMEs with low-risk processing for compliance with proactive responsibility.

- Take into account that most companies are micro-enterprises, SMEs and self-employed workers, and that creating two types of obligations, one for large companies and another for them, is not sufficient to separate some obligations such as the ROPA by number of employees and then make exceptions such as it not being occasional processing. Data protection should be a strict obligation for those who truly put users' data at risk, not a bureaucratic obstacle and yet another brake on entrepreneurship.

Practical application and proactive responsibility

- Improve the practical application of GDPR principles, the application of legal bases, the accreditation of the principle of proactive responsibility, and the exemption from punitive liability if there is no intent or gross negligence. Specify in more detail and avoid vague legal concepts, as well as reduce the deadlines for adopting the proposed measures.

Regulation of the data processor

- Rethink the role of the data processor in cases where the data controller cannot freely decide on the criteria and means of processing because they depend directly on those of the processor, a situation that is all too common when the data controller has no effective decision-making power or because the processor can request or demand processing procedures that are more favourable to them.

Extension of the mandatory need for a DPO

- Extend the circumstances in which a DPO is required whenever there is special data processing such as for criminal, civil or administrative offences, as well as data processing of vulnerable persons or minors.

Professionalisation and Training of Advisors

- Require professionals and companies engaged in personal data protection consulting to be continuously trained, certified, and comply with a code of ethics, whether as DPOs or as simple consultants.

Compatible further processing

- Review of compatible further processing under Article 6.4 of the GDPR.

Public awareness

- Both documents specify their actions in relation to the obligations of the controller/processor, leaving aside public awareness of the fundamental right to data protection.